

WATERMARKING ALGORITHM BASED ON MODIFIED NON-
NEGATIVE MATRIX FACTORIZATION

by

Can KAYACAN

B.S., Electrical & Electronics Engineering, Boğaziçi University, 2003

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Electrical and Electronics Engineering
Boğaziçi University
2008

ACKNOWLEDGEMENTS

I would like to thank my thesis supervisor, Assist. Prof. M. Kıvanç Mihçak for his guidance and motivation throughout my study. Without his assistance, encouragement and suggestions in all stages, this thesis could not have been completed.

Finally, I would like to thank my family for their support during the period of study.

ABSTRACT

WATERMARKING ALGORITHM BASED ON MODIFIED NON-NEGATIVE MATRIX FACTORIZATION

Non-negative matrix factorization has become a significant area of research within the last 10 years. After the research paper "Learning the parts of objects by non-negative matrix factorization" by Daniel D. Lee & H. Sebastian Seung [1] was published, non-negative matrix factorization was applied to many research areas like text mining and image processing.

Since non-negative matrix factorization (NMF) does not provide exact matrix decomposition, iterative methods are being used that depend on many factors like initial conditions and additional constraints that depend on the application requirements. Some of previous researches were aimed to find a unique solution for NMF, on the other hand some of them were based on using NMF with suitable constraints.

This thesis studies the watermarking performance a new NMF algorithm that based on fixing on of the resulting matrixes of NMF algorithm. Within this thesis, the multiplicative NMF algorithm introduced by Daniel D. Lee & H. Sebastian Seung [2] was modified and used for watermarking. The performance of the modified NMF algorithm is analyzed in terms of different parameters with the results of several simulations.

ÖZET

FARKLILAŞTIRILMIŞ NEGATİF OLMAYAN MATRİS AYRIŞTIRMA TEMELLİ İMGE DAMGALAMA ALGORİTMASI

Son on yılda, negatif olmayan matris ayrıştırma (NOMA) önemli bir araştırma alanı haline geldi. Daniel D. Lee & H. Sebastian Seung [1] tarafından yayımlanan “objelerin parçalarını negatif olmayan matris ayrıştırma ile öğrenme” çalışmasının ardından, NOMA veri madenciliği ve imge işleme gibi bir çok araştırma alanında uygulandı.

NOMA kesin ve tek bir matris ayrımı sağlamadığından, NOMA için kullanıldığı uygulama alanının özelliklerine göre değişebilen öncel koşullar ve kısıtlamalara dayalı yinelemeli algoritmik metodlar kullanıldı. Bu metodlardan bazıları kesin bir matris ayrıştırmasını hedeflerken, bazıları kullanıldığı uygulamanın özelliğine uygun kısıtlamaları uygulamayı hedefledi.

Bu tez ile, NOMA sonucunda elde edilen matrislerden birisini sabit tutarak uygulanan yeni bir NOMA metodunun imge damgalama alanındaki performansı incelenmiştir. Bu tez kapsamında Daniel D. Lee & H. Sebastian Seung [2] tarafından ortaya atılan çarpımsal NOMA algoritması temel alınmıştır. Bu yeni metodun performansı değişken parametreler ile yapılan simülasyonlar ile analiz edilmiştir.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	iii
ABSTRACT.....	iv
ÖZET.....	v
LIST OF FIGURES.....	viii
LIST OF TABLES	viii
LIST OF SYMBOLS / ABBREVIATIONS.....	xiv
1. INTRODUCTION.....	1
1.1. Motivation	1
1.2. Outline of the Thesis	2
2. MODIFIED NON-NEGATIVE MATRIX FACTORIZATION ALGORITHM.....	3
2.1. NMF Algorithm.....	3
2.2. Multiplicative NMF Algorithm	3
2.3. Modified NMF Algorithm.....	5
3. WATERMARKING IN NMF DOMAIN.....	7
3.1. Watermark Embedding in NMF Domain.....	8
3.1.1. Watermark Embedding Estimation in Spatial Domain.....	10
3.2. Watermark Verification in NMF Domain.....	11
4. WATERMARKING WITH MULTIPLICATIVE NMF.....	14
4.1. Watermark Embedding with Multiplicative NMF.....	14
4.2. Watermark Verification with Multiplicative NMF.....	15
5. WATERMARKING WITH MULTIPLICATIVE NMF AND SINGULAR VALUE DECOMPOSITION.....	17
5.1. Watermark Embedding with NMF and SVD.....	17
5.2. Watermark Verification with NMF and SVD.....	18
6. WATERMARKING WITH PROPOSED MODIFIED NMF ALGORITHM.....	20
6.1. Watermark Embedding with Modified NMF.....	20
6.2. Watermark Verification with Modified NMF.....	25
7. SIMULATIONS.....	27
7.1. Watermarking Simulations with Modified NMF.....	27
7.1.1. NMF Dimension Related Modified NMF Simulations.....	29

7.1.2. Watermark Power Related Modified NMF Simulations.....	31
7.1.3. AWGN Attack Related Modified NMF Simulations.....	32
7.1.4. JPEG Attack Related Modified NMF Simulations.....	35
7.1.5. Rotation Attack Related Modified NMF Simulations.....	38
7.1.6. Scaling Attack Related Modified NMF Simulations.....	41
7.2. Simulations for Comparison of Watermark Verification Using Multiplicative, NMF-SVD and Modified NMF.....	44
7.2.1. Performance Relations without Any Attack.....	46
7.2.2. AWGN Attack Related Simulations.....	48
7.2.3. JPEG Compression Attack Related Simulations.....	50
7.2.4. Rotation Attack Related Simulations.....	52
7.2.5. Scaling Attack Related Simulations.....	54
8. CONCLUSIONS.....	56
REFERENCES.....	58

LIST OF FIGURES

Figure 3.1. Effect of modification in NMF domain to spatial domain.....	9
Figure 3.2. Watermarking in spatial domain for NMF estimation.....	10
Figure 3.3. Watermarking in spatial domain for NMF estimation.....	11
Figure 3.4. Correlation value distribution at the decoder.....	12
Figure 4.1. Watermark embedding with multiplicative NMF.....	15
Figure 4.2. Watermark verification with multiplicative NMF.....	16
Figure 5.1. Watermark embedding with SVD and NMF.....	18
Figure 5.2. Watermark verification with SVD and NMF.....	19
Figure 6.1. Watermark embedding for modified NMF.....	21
Figure 6.2. Original Lena image size of 512x512.....	23
Figure 6.3. Watermark of PSNR 30 db is embedded via modified NMF.....	23
Figure 6.4. Difference between the original and the watermarked image when watermark of PSNR 30 db is embedded via modified NMF.....	24
Figure 6.5. Watermark of PSNR 25 db is embedded via modified NMF.....	24
Figure 6.6 Difference between the original and the watermarked image when watermark of PSNR 25 db is embedded via modified NMF.....	25

Figure 6.7. Watermark of PSNR 20 db is embedded via modified NMF.....	25
Figure 6.8. Difference between the original and the watermarked image when watermark of PSNR 20 db is embedded via modified NMF.....	26
Figure 6.9. Watermark verification with modified NMF.....	27
Figure 7.1. General simulation overview.....	29
Figure 7.2. ROC curves for modified NMF with different 'r' values when PSNR=20db and no attack is implemented.....	31
Figure 7.3. NMF dimension effect on the accuracy of the watermark verification measured in terms of probability of error.....	31
Figure 7.4. ROC curves for modified NMF with different watermark powers when NMF dimension=35 and no attack is implemented.....	32
Figure 7.5. Watermark power effect on the accuracy of the watermark verification measured in terms of probability of error.....	33
Figure 7.6. ROC curves for modified NMF with dimension=10 and watermark power=30 db is subject to AWGN attacks with different AWGN powers.....	34
Figure 7.7. AWGN power effect on the accuracy of the watermark verification measured in terms of probability of error.....	34
Figure 7.8. ROC curves for modified NMF with different dimensions and watermark power=30 db is subject to AWGN attacks with AWGN power = 18 db...	35
Figure 7.9. ROC curves for modified NMF with dimension=35 and different watermark powers is subject to AWGN attacks.....	36

Figure 7.10. ROC curves for modified NMF with dimension=35 and watermark power=25 db is subject to JPEG compression attacks with different quality factors.....	37
Figure 7.11. JPEG quality effect on the accuracy of the watermark verification measured in terms of probability of error.....	37
Figure 7.12. ROC curves for modified NMF with different NMF dimensions and watermark power=25 db is subject to JPEG compression attacks with quality factor = 90.....	38
Figure 7.13. ROC curves for modified NMF with NMF dimension=35 and different watermark powers is subject to JPEG compression attacks with quality factor = 75.....	39
Figure 7.14. ROC curves for modified NMF with dimension=35 and watermark power=25 db is subject to rotation attacks with different rotation angles.....	40
Figure 7.15. Rotation angle effect on the accuracy of the watermark verification measured in terms of probability of error.....	40
Figure 7.16. ROC curves for modified NMF with different dimension and watermark power=20 db is subject to rotation attacks with rotation angle=1.....	41
Figure 7.17. ROC curves for modified NMF with dimension=35 and different watermark powers is subject to rotation attacks with rotation angle=1.....	41
Figure 7.18. ROC curves for modified NMF with dimension=35 and watermark power=25 db is subject to scaling attacks with different scaling factors.....	42
Figure 7.19. Scaling factor effect on the accuracy of the watermark verification measured in terms of probability of error.....	43

Figure 7.20. ROC curves for modified NMF with different dimensions and watermark power=20 db is subject to scaling attack with scaling factors 0.99.....	43
Figure 7.21. ROC curves for modified NMF with dimension=35 and different watermark powers is subject to scaling attack with scaling factors 0.99.....	44
Figure 7.22. Simulation diagram for algorithms other than modified NMF.....	45
Figure 7.23. ROC curves for different methods when NMF dimension=35 and watermark power=25 db.....	46
Figure 7.24. ROC curves for different methods when NMF dimension=35 and watermark power=30 db.....	47
Figure 7.25. ROC curves for different methods when NMF dimension=35 and watermark power=20 db.....	47
Figure 7.26. ROC curves for different methods when NMF dimension=35 and watermark power=20 db and image is subject to AWGN attack.....	48
Figure 7.27. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to AWGN attack.....	49
Figure 7.28. ROC curves for different methods when NMF dimension=35 and watermark power=30 db and image is subject to AWGN attack.....	49
Figure 7.29. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to JPEG attack of quality=50.....	50

Figure 7.30. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to JPEG attack of quality=75.....	51
Figure 7.31. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to JPEG attack of quality=90.....	51
Figure 7.32. ROC curves for different methods when NMF dimension=35 and watermark power=20 db and image is subject to rotation attack of 1 degree.....	52
Figure 7.33. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to rotation attack of 1 degree.....	53
Figure 7.34. ROC curves for different methods when NMF dimension=35 and watermark power=30 db and image is subject to rotation attack of 1 degree.....	53
Figure 7.35. ROC curves for different methods when NMF dimension=35 and watermark power=20 db and image is subject to scaling attack of scaling factor=0.99.....	54
Figure 7.36. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to scaling attack of scaling factor=0.99.....	55
Figure 7.37. ROC curves for different methods when NMF dimension=35 and watermark power=30 db and image is subject to scaling attack of scaling factor=0.99.....	55

LIST OF TABLES

Table 2.1. Multiplicative NMF Algorithm.....	5
Table 2.2. Modified NMF algorithm.....	6
Table 3.1. Watermark embedding algorithm in NMF domain.....	9
Table 4.1. Watermark embedding algorithm with multiplicative NMF.....	15
Table 4.2. Watermark verification algorithm with multiplicative NMF.....	16
Table 5.1. Watermark embedding algorithm with SVD and NMF.....	17
Table 5.2. Watermark verification algorithm with SVD and NMF.....	19
Table 6.1. Watermark embedding algorithm for Modified NMF.....	20
Table 6.2. Watermark verification algorithm with modified NMF.....	26

LIST OF SYMBOLS / ABBREVIATION

AWGN	Additive white gaussian noise
E	Error matrix
H	Coefficient matrix of NMF decomposition
H_i	Initial H matrix
H^k	Modified H matrix
H_m	Watermarked H matrix
H_M	H matrix of NMF decomposition of watermark
H_r	H matrix recovered at the receiver
JPEG	Joint Photographic Experts Group
M	Watermark
MSE	Mean squared error
n	Noise
NMF	Non-negative matrix factorization
P_e	Probability of error
PFA	Probability of false alarm
PMiss	Probability of miss
PSNR	Peak signal to noise ratio
r	NMF dimension
RMSE	Root mean squared error
ROC	Region of convergence
SVD	Singular value decomposition
T_{Hi}	Unitary matrix of SVD of initial H matrix
T_{HM}	Unitary matrix of SVD of H matrix of watermark NMF decomposition
U_{Hi}	Unitary matrix of SVD of initial H matrix
U_{HM}	Unitary matrix of SVD of H matrix of watermark NMF decomposition
V	Cover image
V_m	Watermarked cover image
V_r	Received cover image
W	Basis matrix of NMF decomposition

W_i	Initial W matrix
W^k	Modified W matrix
W_m	Watermarked W matrix
W_M	W matrix of NMF decomposition of watermark
W_r	W matrix recovered at the receiver
X	Arbitrary matrix
X^{-1}	Inverse of arbitrary matrix
Z_{Hi}	Diagonal matrix of SVD of initial H matrix of V_r
Z_{HM}	Diagonal matrix of SVD of initial H matrix of watermark
Z_m	Watermarked diagonal matrix of SVD
Γ	Threshold

1. INTRODUCTION

1.1. Motivation

Non-negative matrix factorization (NMF) has gained much attention over the past decade. This has been due to the increasing usage of NMF within various research areas.

The first concept of NMF was introduced by P. Paatero & U. Tapper [3] in 1994. Although this study deals with positive matrix factorization, it is accepted as the ancestor of the NMF. The non-negativity constraint provides a physical correlation since all the physical entities are non-negative. That is, in order to decompose a physical object like an image in to addition of various images or entities, NMF provides a logical method. The study of Daniel D. Lee & H. Sebastian Seung [1] provides the result that if a facial image is decomposed via NMF the resulting decomposition looks like facial elements like nose, eyes and ears. Another advantage is to create sparse matrices compared to other decomposition algorithms like singular value decomposition (SVD).

Despite its advantages NMF has some disadvantages [4]. The most significant disadvantage is the fact that NMF does not have a unique solution. Another significant disadvantage is the transformation between the spatial domain and NMF domain. Although the transformation between domains is rather difficult the NMF domain is proved to be robust a domain in terms of image processing like hashing [5].

In this thesis, the focus is on the watermarking in the NMF domain. However due to the transformation difficulties, instead of embedding watermark in the NMF domain, the watermark embedded image is estimated in the spatial domain to simulate the watermarked image in the NMF domain. To start with the basic model the multiplicative NMF model is modified in terms of fixing one of the matrices.

The motivation of the thesis is to study the performance possibilities of using modified NMF for image watermarking under several attacks and compare the performance results with several algorithms.

1.2. Outline of the Thesis

The thesis is organized as follows: basic concept of NMF is explained, multiplicative NMF and modified NMF are introduced in Chapter 2.

In Chapter 3, watermarking concepts and watermarking in NMF domain is analyzed. Watermarking estimation in the spatial domain is also examined.

Watermarking using multiplicative NMF, embedding and verification methods are studied in Chapter 4.

Chapter 5 introduces the watermarking method based on NMF-SVD model and the algorithm structure is analyzed.

In Chapter 6, the newly introduced modified NMF algorithm is examined in detail. The watermarking mechanism with modified NMF is also analyzed in this chapter.

Simulations for both newly proposed modified NMF and other algorithms are provided and analyzed in Chapter 7.

Chapter 8 concludes the thesis emphasizing the results of watermarking based on modified NMF simulations also mentioning some suggestions for future work on this subject.

2. MODIFIED NON-NEGATIVE MATRIX FACTORIZATION ALGORITHM

2.1. NMF Algorithm

NMF was first introduced by Paatero & U. Tapper [3] in 1994 as positive matrix factorization. Due to the fact that, NMF is not an exact decomposition many algorithms have been introduced. Although the most popular one is the multiplicative algorithm [2], there are some other studies based on different constraints [7] and different iterative methods like gradient descent [8]. Since NMF is an iterative algorithm, the decomposition depends on the initialization and iterative methods used for NMF algorithm. There are also several researches that analyze different NMF methods and different factors affecting NMF decomposition [4,6].

2.2. Multiplicative NMF Algorithm

Multiplicative NMF algorithm was introduced by Daniel D. Lee & H. Sebastian Seung in 2001 [2]. This algorithm constructs the basis for proceeding researches. The main advantage is that it guarantees the non-negativity constraint due to its multiplicative rule.

NMF algorithm is used to solve the following equation:

$$V = W * H \tag{2.1}$$

where V is a non-negative $m \times n$ matrix, W is a $m \times r$ matrix and H is a non-negative $r \times n$ matrix. “ r ” can be considered as a factorization rank for NMF. Different NMF factorization ranks are analyzed in this thesis.

However, this equation does not have a unique solution.

$$W^k = W * X \tag{2.2}$$

$$H^k = X^{-1} * H \tag{2.3}$$

$$W^k * H^k = (W * X) * (X^{-1} * H) \quad (2.4)$$

$$W^k * H^k = W * (X * X^{-1}) * H \quad (2.5)$$

$$W^k * H^k = W * I * H = W * H \quad (2.6)$$

$$V = W * H = W^k * H^k \quad (2.7)$$

Due to estimation there exists an error term as:

$$V = W * H + E \quad (2.8)$$

To minimize the error term E, the Euclidian distance is between the cover image V and the multiplication of the resulting matrices of the NMF algorithm is constrained to be minimum:

$$\text{Min}(\|V - W * H\|) \text{ with respect to } W \text{ and } H, \text{ subject to the constraints } W_{ij}; H_{ij} \geq 0 \text{ for all } i,j \quad (2.9)$$

In order to solve 2.9 the following steps are followed:

$$\|V - W * H\| = (V - W * H) * (V - W * H)^T \quad (2.10)$$

The resulting update rules are:

$$H_{a\mu} \leftarrow H_{a\mu} \frac{(W^T V)_{a\mu}}{(W^T W H)_{a\mu}} \quad W_{ia} \leftarrow W_{ia} \frac{(V H^T)_{ia}}{(W H H^T)_{ia}} \quad (2.11)$$

Instead of using the Euclidean distance (2.9), the multiplicative NMF can be constrained on the divergence as [2]:

$$D(A||B) = \sum_{ij} \left(A_{ij} \log \frac{A_{ij}}{B_{ij}} - A_{ij} + B_{ij} \right) \quad (2.12)$$

Table 2.1. Multiplicative NMF Algorithm [2]

Step 1: Initialize W

Step 2: Initialize H

Step 3: Update H as:

$$H_{i+1} = H_i * [(W_i^T * V) / (W_i^T * W_i * H_i)] \quad (2.13)$$

Step 4: Update W as:

$$W_{i+1} = W_i * [(V * H_i^T) / (W_i * H_i * H_i^T)] \quad (2.14)$$

Step 5: Verify convergence for H as the mean of the difference matrix of H:

$$\text{mean2}(H_{i+1} - H_i) < \text{Threshold}$$

The resulting update rules based on (2.12) are:

$$H_{a\mu} \leftarrow H_{a\mu} \frac{\sum_i W_{ia} V_{i\mu} / (WH)_{i\mu}}{\sum_k W_{ka}} \quad W_{ia} \leftarrow W_{ia} \frac{\sum_\mu H_{a\mu} V_{i\mu} / (WH)_{i\mu}}{\sum_\nu H_{a\nu}} \quad (2.15)$$

Since this a multiplicative update algorithm, this guarantees the non-negativity that is a problem for additive or gradient update rules [6]. This algorithm is the basis for other algorithms. There exist other algorithms that base on gradient descent [8] or additional constraints like sparseness [7]. This thesis studies the NMF algorithm introduced in 2001 [2] and the details are provided above.

2.3. Modified NMF

In this thesis, a modified NMF algorithm is analyzed. The analyzed modified algorithm bases on the multiplicative NMF algorithm. However instead of using the multiplicative NMF algorithm that iterates on both matrices W and H, W is kept fixed in the proposed modified NMF algorithm. This gives us the advantage of using the fixed matrix W as a secret key. Since NMF is sensitive to the initial conditions [4], using a specific initial matrix W and not updating it, results in a decomposition unique to that

initial and not updated W . Moreover keeping one of the matrices fixed in the NMF algorithm reduces the computation time.

The NMF algorithm treats the columns of W as the basis components and H is the combination matrix for these components. With the modified NMF algorithm, the basis components are fixed, that is the aim can be considered as finding the non-negative combination factors of the predetermined basis components.

Table 2.2. Modified NMF algorithm

Step 1: Initialize W

Step 2: Initialize H

Step 3: Update H as:

$$H_{i+1} = H_i * [(W_i^T * V) / (W_i^T * W_i * H_i)] \quad (2.16)$$

Step 4: Verify convergence for H as the mean of the difference matrix of H :

$$\text{mean2}(H_{i+1} - H_i) < \text{Treshold}$$

3. WATERMARKING IN NMF DOMAIN

Watermarking is an important issue in the field of multimedia security protection. Especially in the image security concerns it is a widely used method. It is a technique that the image is processed with an invisible seal (watermark) that cannot be realized perceptually. Within several techniques this watermark can be recovered from the processed image in order to determine the copyright owner of the image. There are several methods for watermarking however these are some common constraints while building up a watermarking method [9]:

- *Unobtrusiveness*: The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.
- *Robustness*: The watermark should be difficult to remove. Mostly, the watermark should be robust in the following operations:
 - *Common signal processing*: The watermark should still be recoverable even if common signal processing operations are applied to the image. These include common signal enhancements to image contrast and color and compressions for example.
 - *Common geometric distortions*: Watermarks in image should also be resilient to geometric image operations, such as rotation and resizing that are expected not to disturb the whole perceptual orientation of the image.
- *Unambiguousness*: Recovery of the watermark should identify the owner of the image. Moreover this identification should be immune to the various attacks that are explained above.

The two basic watermarking methods can be summarized as:

- *Spread Spectrum*: In this watermarking technique the watermark is distributed over the whole frequency spectrum randomly instead of just using the high frequency components which results in more secure watermark [9].
- *Quantization Index Modulation*: Quantization index modulation refers to embedding information by first modulating an index or sequence of indices with the embedded information and then quantizing the host signal with the associated quantizer or sequence of quantizers [12]. This process can be also performed in a randomized manner (i.e., in a domain which is obtained via applying a pseudo-random transform to the input image) in order to gain robustness against the possible attacks, especially the ones that are designed by an intelligent adversary [10].

Although the methods used for watermark embedding and verification differ in many aspects, in this thesis the NMF effect is placed in the first place for a basic watermarking embedding and verification algorithm as a direct addition of watermark to the cover image.

3.1. Watermark Embedding in NMF Domain

After it was verified that NMF domain is robust for hashing, the motivation has been emerged for the usage of NMF for image watermarking [5]. However instead of using directly multiplicative NMF, modified NMF introduces more security since matrix W is fixed and can be considered as a secret key. Previously NMF was used for watermarking in other researches [11].

In this thesis, watermarking based on modified NMF is compared with two other proposed algorithms: watermarking via multiplicative NMF and watermarking via NMF and SVD [11].

In order to make use of the the advantages of the NMF domain in terms of image watermarking, the following algorithm is constructed:

Table 3.1. Watermark embedding algorithm in NMF domain

- Step 1: Apply NMF to initial image V and get the initial matrices W_i and H_i
- Step 2: Embed watermark to W_i and get W_m
- Step 3: Obtain the watermarked image V_m as $V_m = W_m * H_i$
- Step 4: Apply NMF to watermarked image V_m to get W_m for watermark verification

Although NMF domain is robust, watermark embedding in NMF domain is not much convenient. The reason is that the small deviation in spatial domain results in a bigger diversion in the NMF domain that makes it hard to verify or recover the embedded watermark.

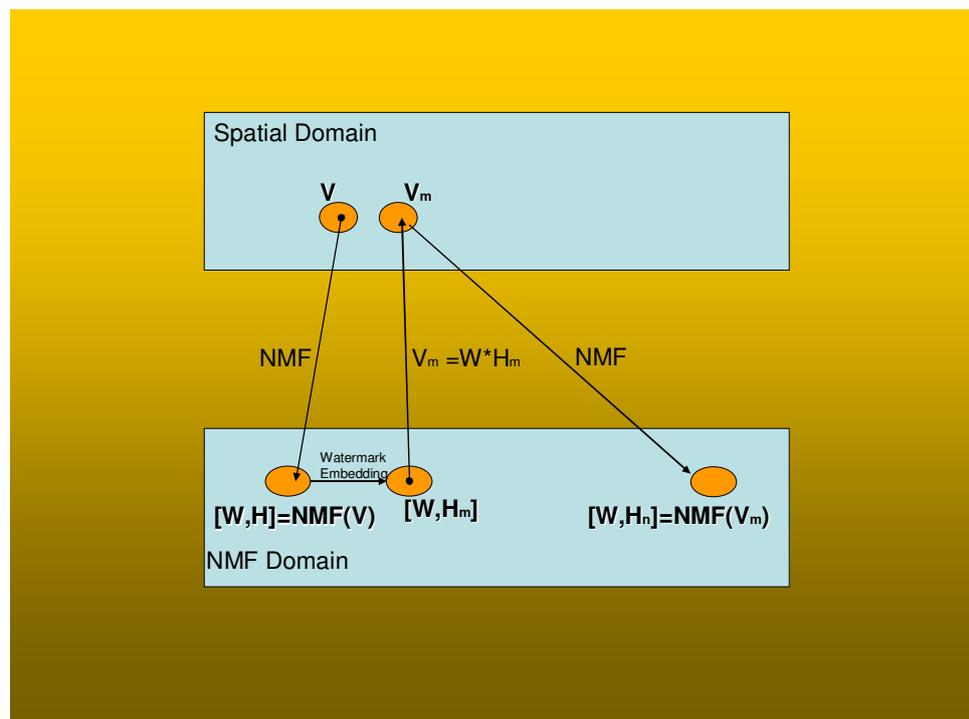


Figure 3.1. Effect of modification in NMF domain to spatial domain

This result gives the intuition that instead of embedding the watermark to the in the NMF domain, the watermarked image should be estimated in the spatial domain to give the watermarked H matrix in the NMF domain after NMF is applied to watermarked image.

3.1.1. Watermark Embedding Estimation in Spatial Domain

NMF is a nonlinear operation, due to its iterative nonlinear algorithm. In order to model the watermark embedding effect in the NMF domain to the spatial domain, (2.1) is estimated to be a linear equation due to the fact that W is fixed, despite the fact that NMF itself is a nonlinear operation. This estimation results in the following set of equations:

$$V = W * H \quad (3.1)$$

$$H_m = H + M \quad (3.2)$$

$$V_m = W * H_m \quad (3.3)$$

$$V_m = W * (H + M) \quad (3.4)$$

$$V_m = W * H + W * M \quad (3.5)$$

$$V_m = V + W * M \quad (3.6)$$

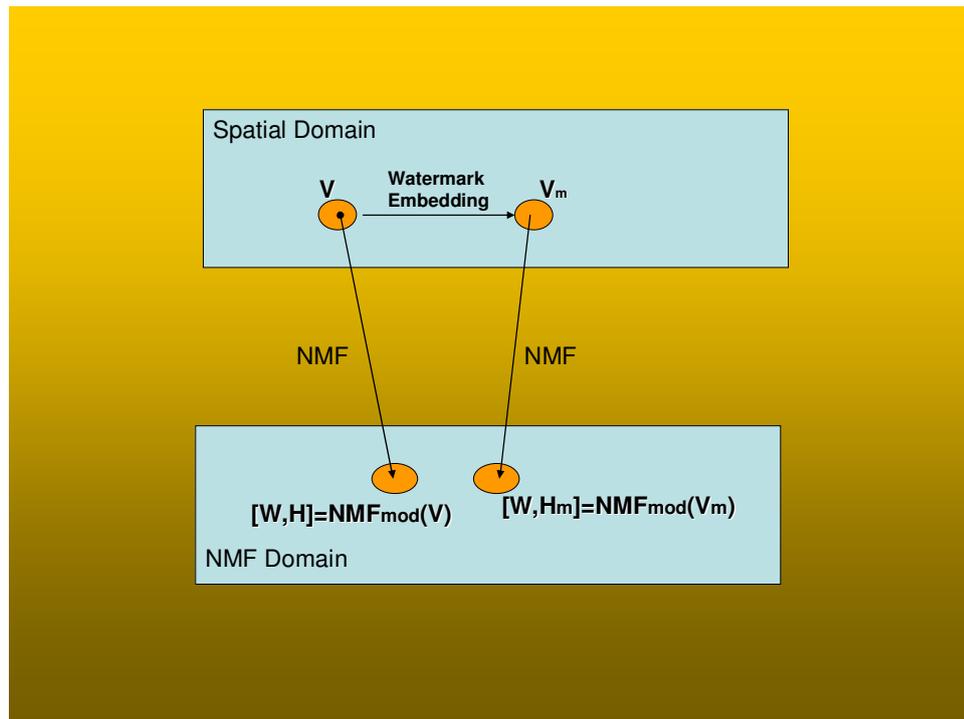


Figure 3.2. Watermarking in spatial domain for NMF estimation

As described in Figure 3.2 the watermarked is embedded in the spatial domain and it is expected to have a correlation between the resulting watermarked matrix H_m and watermark. This correlation is the basis of the watermark detection mechanism that is going to be proposed in the following sections.

3.2. Watermark Verification in NMF Domain

As the second step of the watermarking procedure, the watermark has to be recovered and verified correctly for copyright ownership. The watermark verification mechanism is based on the correlation between the watermark and the coefficient matrix H that is produced as the result of NMF algorithm.

The main idea of correlation can be expressed as:

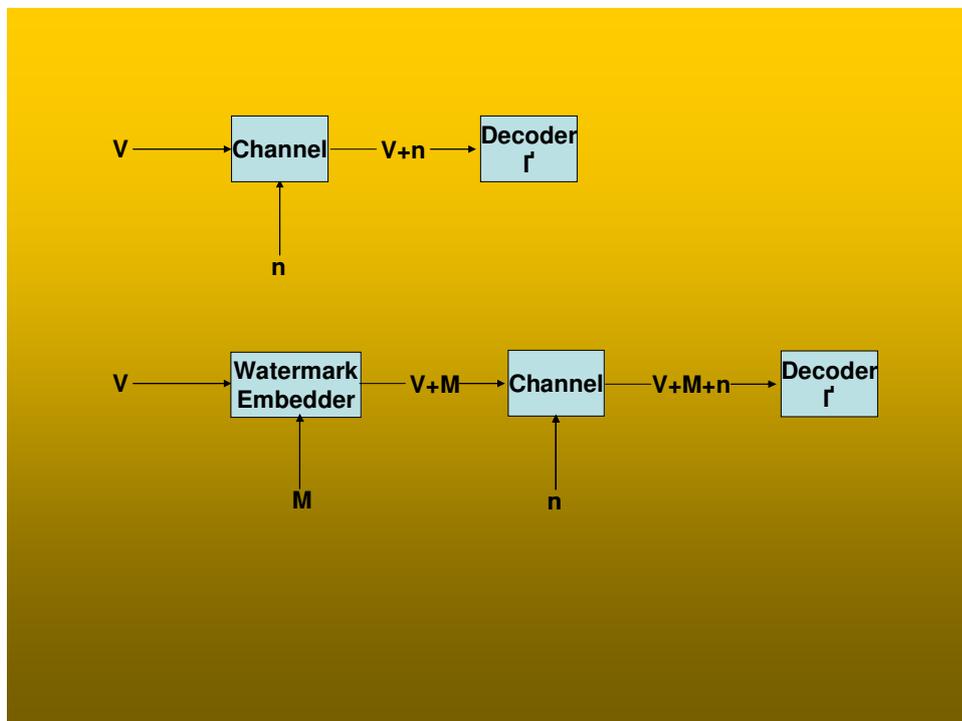


Figure 3.3. Watermark embedding and verification flow

In order to calculate the correlation between H and the watermark normalized correlation is used as:

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}} \quad (3.7)$$

where $\bar{A} = \text{mean2}(A)$, and $\bar{B} = \text{mean2}(B)$.

The watermark verification is done according to this normalized correlation value. The obtained normalized correlation value is compared with the threshold value.

$$\text{Corr}(V+M+n, M) = \text{Corr}(V+n, M) + E(\|M\|)^2 \quad (3.8)$$

According to (3.8) the watermarked image and the not watermarked image can be distinguished via the $E(\|M\|)^2$ difference.

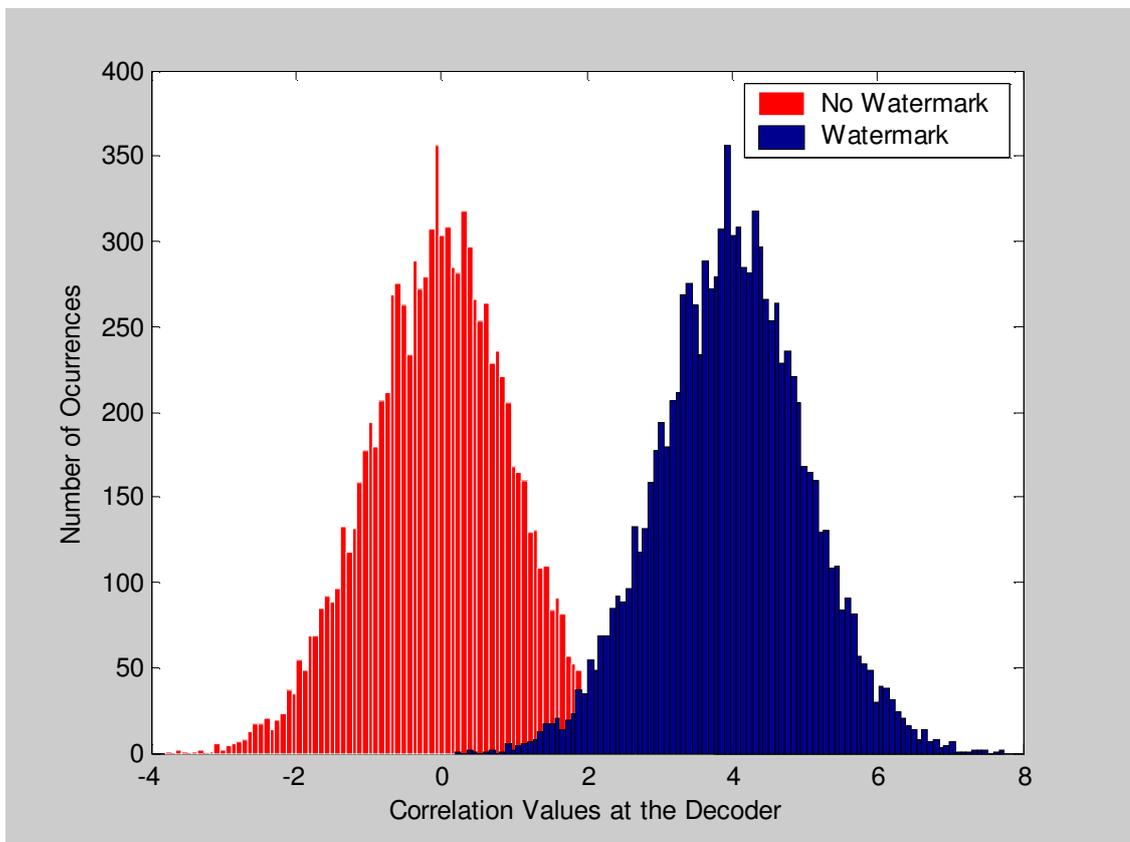


Figure 3.4. Correlation value distribution at the decoder

The difference value can also be seen from Figure 3.4 above. These values above a certain threshold imply watermark is present and values below the threshold imply no watermark is present. However there will be some values that match a false alarm that is the correlation value is higher than the threshold but no watermark is present and there will be some values that match a miss of watermark that is the correlation value is lower than the threshold value but the watermark exists.

In this thesis, this concept of watermark verification is used. However in the decoder the correlation is performed in the NMF domain that is the correlation between the resulting H matrix of NMF algorithm and watermark M is taken into account for verification.

4. WATERMARKING WITH MULTIPLICATIVE NMF

There are several watermarking and NMF algorithms proposed by different researchers. In this thesis, the main focus is on the newly proposed modified NMF algorithm in which instead of modifying both W and H matrices throughout the iterations, only H matrix is updated and W matrix is kept unchanged. However other than the modified algorithm, multiplicative NMF and singular value decomposition (SVD) - NMF based watermarking are also analyzed within this thesis.

4.1. Watermark Embedding with Multiplicative NMF

The multiplicative NMF algorithm [2] is analyzed in section 2.2. It provides the basis for most of the NMF algorithms. There are two cost functions for this algorithm as Euclidean distance and divergence, in this thesis Euclidean distance is used as a cost function.

Due to the reasons provided in section 3.1 watermark is embedded in spatial domain to estimate the effect in the NMF domain as:

$$V_m = V + (W * M) \quad (4.1)$$

In order to embed the watermark the W matrix has be produced as a result of multiplicative NMF. After getting the W matrix watermark can be embedded as (4.1). After embedding the watermark to the cover image as in Figure 4.1, the watermarked image passes through the channel and finally it is received at the decoder part of the receiver in order to be verified.

The watermark embedding algorithm with multiplicative NMF can be summarized as follows:

Table 4.1. Watermark embedding algorithm with multiplicative NMF

<p>Step 1: Apply multiplicative NMF to cover image V and get the initial matrices W_i and H_i</p> <p>Step 2: Embed watermark to V and get V_m as $V_m = V + (W_i * M)$</p>
--

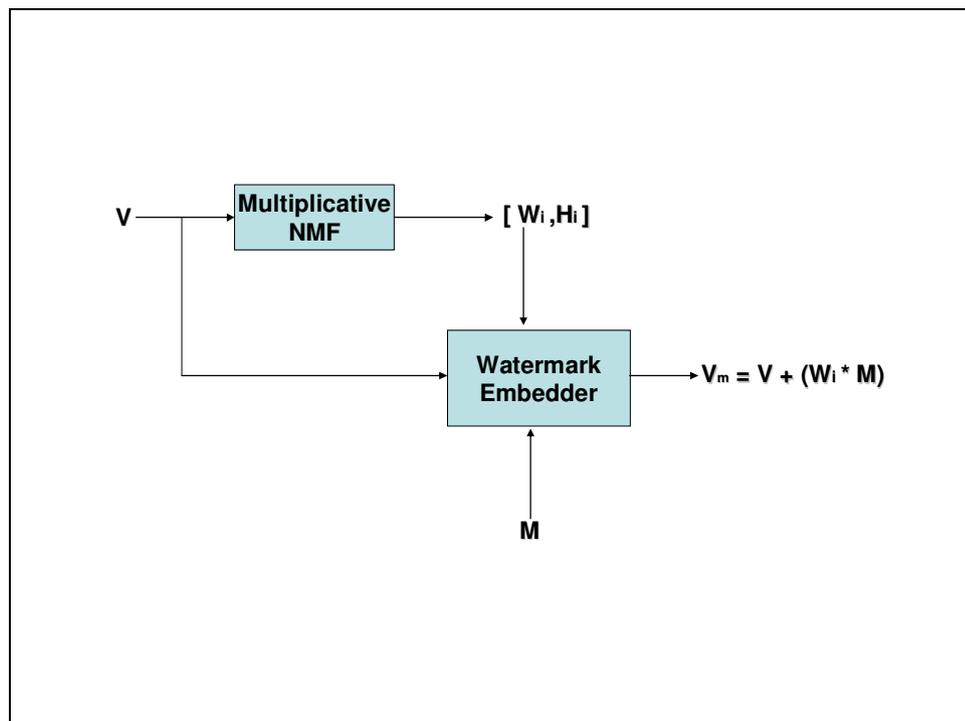


Figure 4.1. Watermark embedding with multiplicative NMF

4.2. Watermark Verification with Multiplicative NMF

After the image is received at the decoder as in Figure 3.3 the watermark verification procedure is applied to the received image. The verification procedure is based on the comparison between the threshold value and the correlation value of H matrix that results from the multiplicative NMF and the watermark. In order to correlate the watermark and H matrix, first H matrix has to be produced via multiplicative NMF with the same initial conditions that are used for the watermark embedding.

Table 4.2. Watermark verification algorithm with multiplicative NMF

<p>Step 1: Apply multiplicative NMF to received image V_r and get the received matrices W_r and H_r</p> <p>Step 2: Calculate the correlation between H_r and watermark M as $\text{Corr}(H_r, M)$</p> <p>Step 3: Compare the correlation value with the threshold value</p> <p>Step 4: If $\text{Corr}(H_r, M) \geq \text{Threshold}$, then watermark is present</p> <p>Step 5: If $\text{Corr}(H_r, M) < \text{Threshold}$, then no watermark is present</p>
--

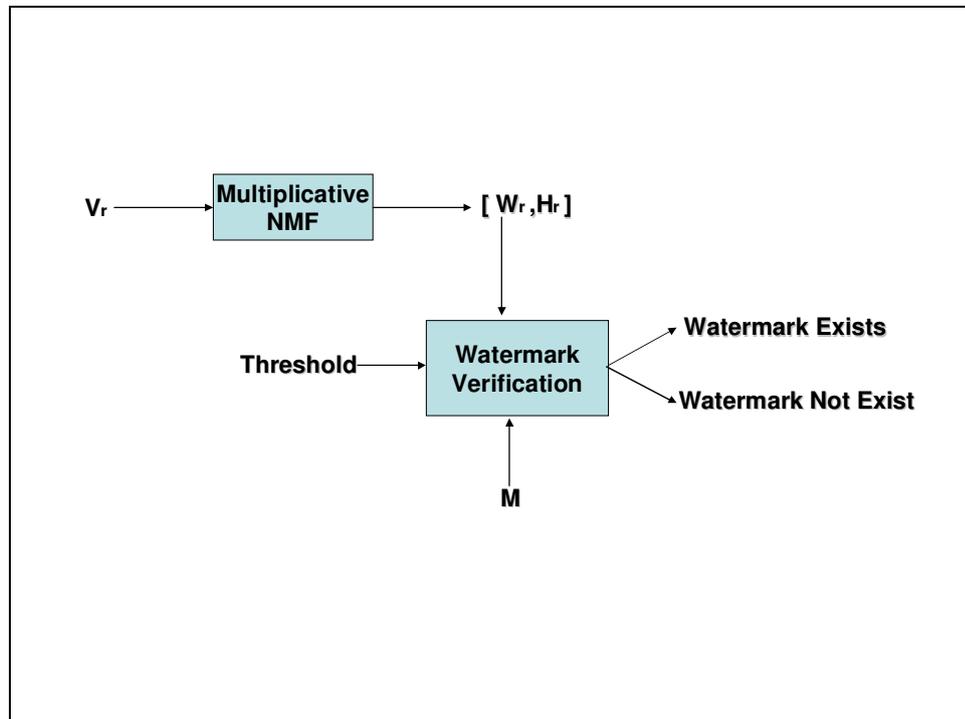


Figure 4.2. Watermark verification with multiplicative NMF

5. WATERMARKING WITH MULTIPLICATIVE NMF AND SINGULAR VALUE DECOMPOSITION

A recent watermarking approach using NMF is introduced by M. Ghaderpanah and A. B. Hamza in 2006 [11]. This approach involves SVD together with NMF. The image is first gone through NMF than SVD is applied to the resulting H matrix. Multiplicative NMF is also used for this watermarking method. Watermark embedding and verification is provided in the following sections.

5.1. Watermark Embedding with NMF and SVD

The main idea is to apply first NMF to cover image and the watermark. Then apply SVD to both H matrices that are produced from the NMF of cover image and watermark. The addition of the diagonal matrices gained from SVD provides the basis of the watermarked image. In order to construct the watermarked image the matrices obtained from the cover image and the matrix obtained from the addition is used.

The algorithm for the watermark embedding with NMF and SVD can be constructed as:

Table 5.1. Watermark embedding algorithm with SVD and NMF

<p>Step 1: Apply multiplicative NMF to cover image V and get the initial matrices W_i and H_i</p> <p>Step 2: Apply multiplicative NMF to watermark M and get the watermark matrices W_M and H_M</p> <p>Step 3: Apply SVD to H_i and get U_{Hi}, Z_{Hi}, T_{Hi}</p> <p>Step 4: Apply SVD to H_M and get U_{HM}, Z_{HM}, T_{HM}</p> <p>Step 5: Calculate $Z_m = Z_{Hi} + Z_{HM}$</p> <p>Step 6: Get $V_m = U_{Hi} * Z_m * T_{Hi}^T$</p>

As expected this algorithm that involves both NMF and SVD takes more time to embed the watermark since it involves more steps and operations during embedding as seen in Figure 5.1.

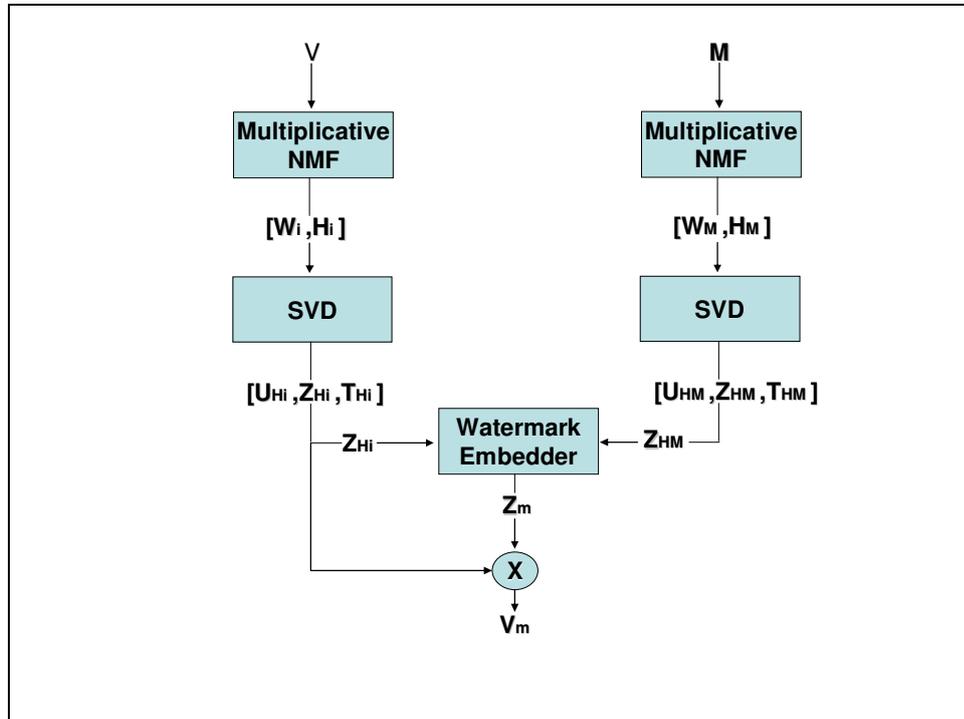


Figure 5.1. Watermark embedding with SVD and NMF

5.2. Watermark Verification with NMF and SVD

Similar to watermark verification with multiplicative NMF, verification procedure bases on the correlation between the H matrix recovered by NMF and the watermark. The initial conditions are kept same as the watermark embedding procedure. The verification depends on the comparison of the threshold and the correlation value of the watermark and the recovered H matrix at the receiver.

The algorithm for watermark verification with multiplicative NMF and SVD based watermarking can be summarized as:

Table 5.2. Watermark verification algorithm with SVD and NMF

<p>Step 1: Apply multiplicative NMF to received image V_r and get the received matrices W_r and H_r</p> <p>Step 2: Calculate the correlation between H_r and watermark M as $\text{Corr}(H_r, M)$</p> <p>Step 3: Compare the correlation value with the threshold value</p> <p>Step 4: If $\text{Corr}([U_{Hi}*(Z_{Hi}+Z_{HM})*T_{Hi}^T], [U_{HM}*Z_{HM}*T_{HM}^T]) \geq \text{Threshold}$, then watermark is present</p> <p>Step 5: If $\text{Corr}([U_{Hi}*(Z_{Hi}+Z_{HM})*T_{Hi}^T], [U_{HM}*Z_{HM}*T_{HM}^T]) < \text{Threshold}$, then no watermark is present</p>
--

In [11], the watermark verification is also based on SVD and NMF. However in this thesis to compare the performance in terms of verification the watermark verification algorithm is based on only NMF and correlation as expressed in Figure (5.2).

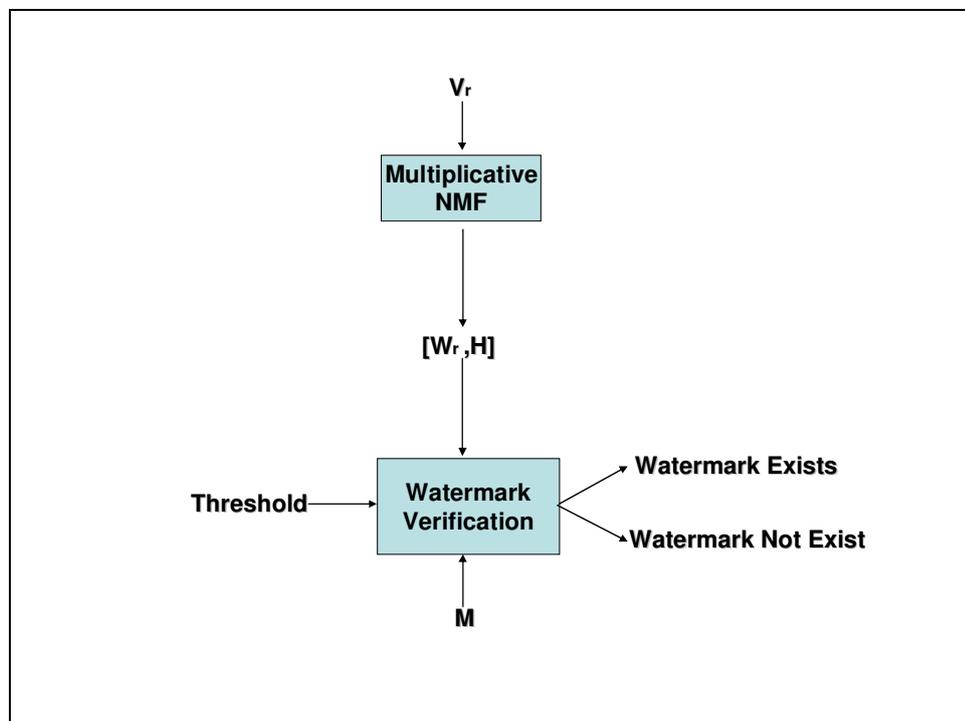


Figure 5.2. Watermark verification with SVD and NMF

6. WATERMARKING WITH PROPOSED MODIFIED NMF ALGORITHM

The main focus in this thesis is on the newly proposed modified NMF algorithm where only H , the coefficient matrix is updated with the multiplicative NMF. During the iterations W is kept unmodified. The watermarking mechanism is similar to watermarking algorithm based on multiplicative NMF and watermarking algorithm based on NMF and SVD. Despite these two, there is no need for a calculation of NMF in the watermark embedding stage. The details are given in section 6.1 and 6.2.

6.1. Watermark Embedding with Modified NMF

Watermark embedding for the modified NMF is similar to other two algorithms. However in the other two algorithms since the basis matrix W has to be obtained prior to watermark embedding, multiplicative NMF algorithm has to be run before watermark embedding. Since with the modified NMF, W is fixed within the algorithm the watermark is directly added to the cover image in the spatial domain. This fact, as expected, decreases the time required for the watermark embedding.

The watermarking embedding algorithm for modified NMF can be summarized as Table 6.1.

Table 6.1. Watermark embedding algorithm for Modified NMF

Step 1: Create the fixed W matrix

Step 2: Get the watermarked image V_m as $V_m = V + (W * M)$

The watermark embedding for modified NMF can be demonstrated as Figure 6.1.

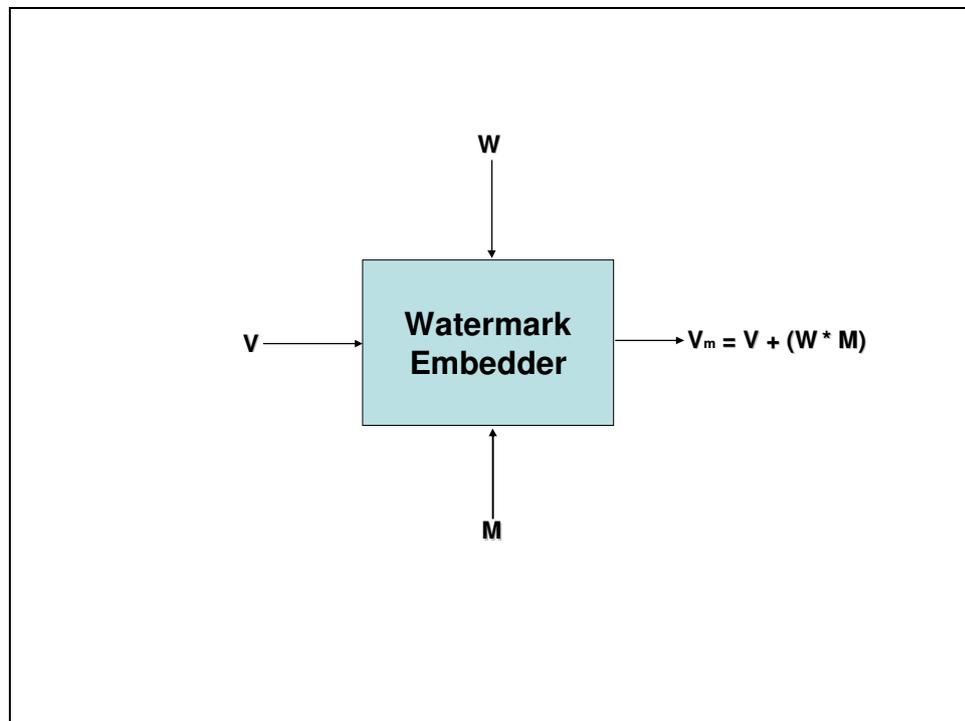


Figure 6.1. Watermark embedding for modified NMF

In order to illustrate the watermark embedding to an image spatially, watermark with various powers are embedded to Lena image of size 512. The distortion is also between the watermarked image and the original image is presented by multiplying the difference between two images by 10 and then put on a pedestal of 128.



Figure 6.2. Original Lena image size of 512x512



Figure 6.3. Watermark of PSNR 30 db is embedded via modified NMF

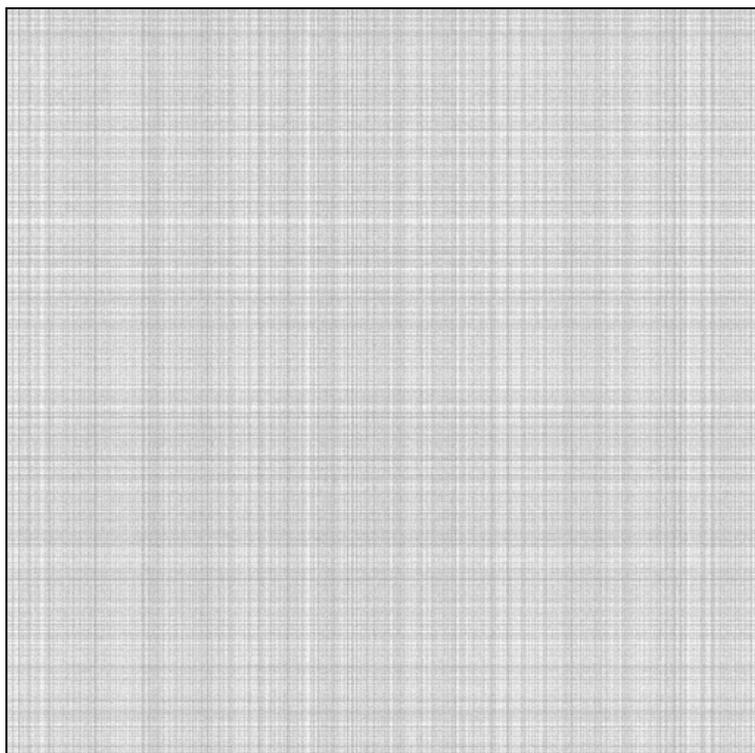


Figure 6.4. Difference between the original and the watermarked image when watermark of PSNR 30 db is embedded via modified NMF



Figure 6.5. Watermark of PSNR 25 db is embedded via modified NMF

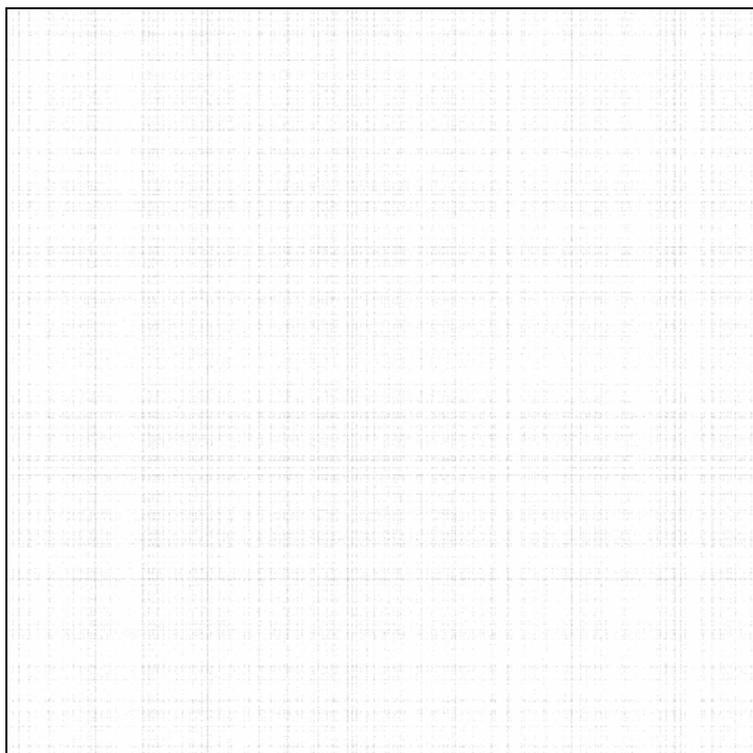


Figure 6.6 Difference between the original and the watermarked image when watermark of PSNR 25 db is embedded via modified NMF



Figure 6.7. Watermark of PSNR 20 db is embedded via modified NMF

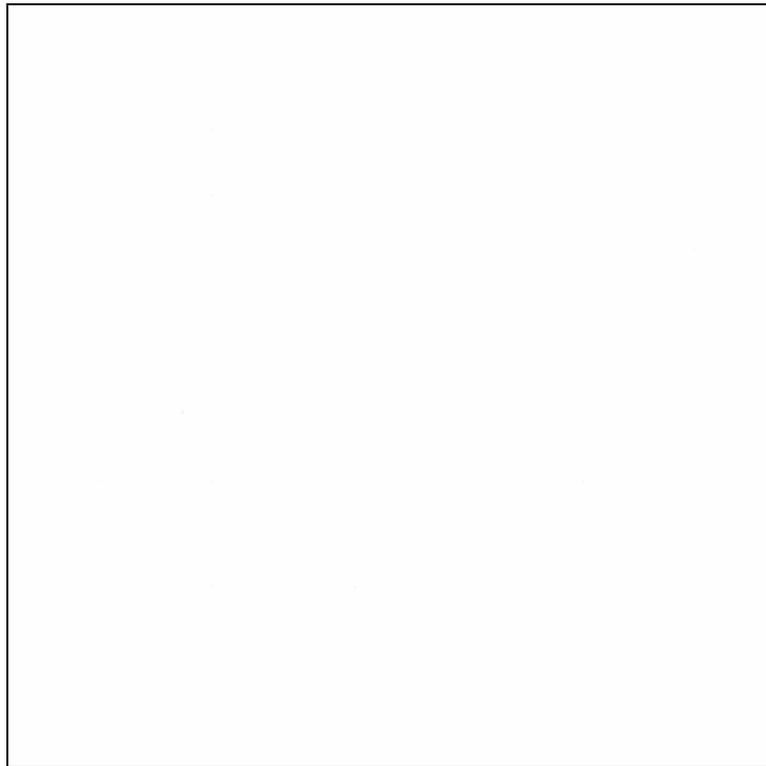


Figure 6.8. Difference between the original and the watermarked image when watermark of PSNR 20 db is embedded via modified NMF completely white due to high pixel values

6.2. Watermark Verification with Modified NMF

After embedding the watermark to the cover image at the sender, the watermark has to be verified at the receiver. Modified NMF is used for watermark verification. Similar to watermark verification with multiplicative NMF, modified NMF is applied to the received image. Since W matrix is fixed within the modified NMF algorithm it is produced with the same parameters at the receiver for verification. Figure 6.9 provides the overview of the verification mechanism.

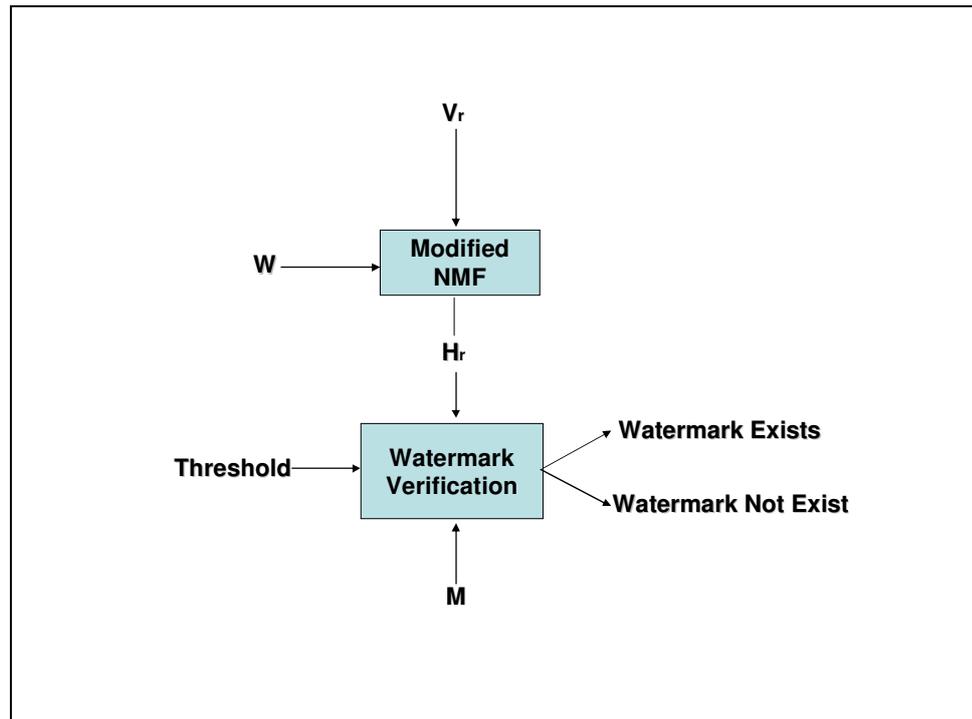


Figure 6.9. Watermark verification with modified NMF

The existence of watermark is identified depending on the correlation value of the watermark and the H matrix obtained by the modified NMF. The normalized correlation is used for this operation.

Table 6.2. Watermark verification algorithm with modified NMF

- Step 1: Apply modified NMF to received image V_r and get the received matrix H_r
- Step 2: Calculate the correlation between H_r and watermark M as $\text{Corr}(H_r, M)$
- Step 3: Compare the correlation value with the threshold value
- Step 4: If $\text{Corr}(H_r, M) \geq \text{Threshold}$, then watermark is present
- Step 5: If $\text{Corr}(H_r, M) < \text{Threshold}$, then no watermark is present

7. SIMULATIONS

7.1. Watermarking Simulations with Modified NMF

There are different factors that affect the NMF algorithm and the watermarking method involving NMF. The performance of watermarking with NMF depends on these factors. In order to identify the effect of these factors simulations has been performed with different values for watermarking with modified NMF.

The simulation bed consists of 3000 gray scale images. The size of all images is 512x512. However all the images pass through a scaling procedure to check whether the image is a 512x512 image. If the image is not a 512x512 image, the scaling procedure scales the image to 512x512 with Matlab function `imresize()`. The `imresize` function is used with 'bicubic' parameter when scaling. For the simulations Matlab Version 6.5.0.180913a Release13 is used.

The simulation environment consists of two separate blocks as sender and receiver as seen in Figure 7.1.

In the sender block, watermark embedding is applied to the cover image. The procedure and algorithm is explained in detail at sections 6.1. To use the same W and keep the initial conditions unchanged the W and the initial matrices are generated with the same secret key for Matlab function `rand`. Since `rand` function generates the numbers in $[0,1]$, the fulfillment of non-negativity constraint is guaranteed for the initial matrices.

The algorithm and the procedure for receiver block has been described in section 6.2. Modified NMF has been used in order to generate H_r matrix, so that normalized correlation can be used for detection of watermark. The normalized correlation is calculated via `corr2` function of Matlab (3.7).

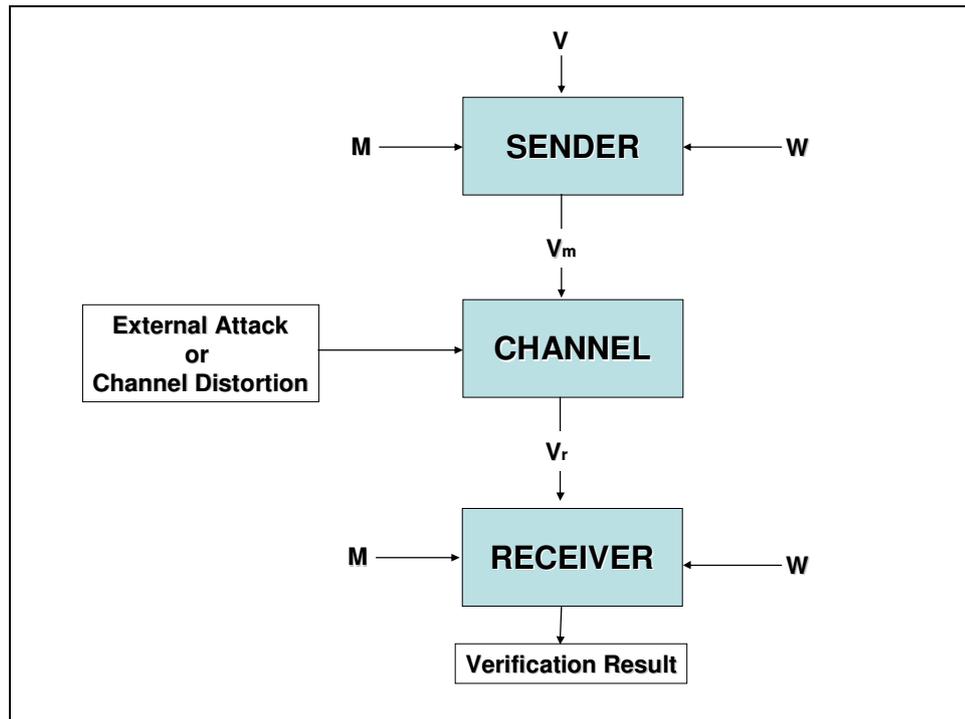


Figure 7.1. General simulation overview

The channel is also simulated with different types. The simulations are channel distortion or external image attacks. The following attacks are applied with different parameters to the watermarked image:

- No Attack
- Additive White Gaussian Noise (AWGN)
- JPEG Compression
- Rotation
- Scaling

NMF is a matrix decomposition in the first place. However it is also a dimension reduction. As explained in section 2.2 the ‘r’ can be considered a dimension reduction parameter and has an effect on the performance of the modified NMF algorithm. The different values of ‘r’ are also considered in the simulations.

Another important parameter for the watermarking simulations is the watermark power. It is certain that watermark power has a great effect on the performance of the modified NMF method. It is expected to have more verification accuracies for the

watermarks that have greater powers. However according to the general watermarking constraints the watermark should not disturb the cover image perceptually. Since, the greater the watermark power, the power of the watermark should be appropriate with regard to cover image. This value is measured with peak signal-to-noise ratio (PSNR) where for images it can be calculated with mean squared error (MSE) and root mean squared error (RMSE). Since the simulation bed consists of images with size 512x512, size of the images (N) is set to 512 for the simulations.

$$\text{MSE} = \frac{\sum [f(i,j) - F(i,j)]^2}{N^2} \quad (7.1)$$

$$\text{PSNR} = 20 \log_{10} \left(\frac{255}{\text{RMSE}} \right) \quad (7.2)$$

7.1.1. NMF Dimension Related Modified NMF Simulations

Like other matrix decompositions modified NMF deals with the dimension reduction. It is certain that with larger matrices the iterations take longer times. However it is found out that the dimension of the modified NMF algorithm affects the performance of the watermark verification. It can be realized from Figure 7.2 that there is no direct correlation between the dimension of NMF and the watermark verification performance. It is observed that the optimum value of the NMF dimension is about 30-50. Due to this fact NMF dimension of 35 is used for other simulations.

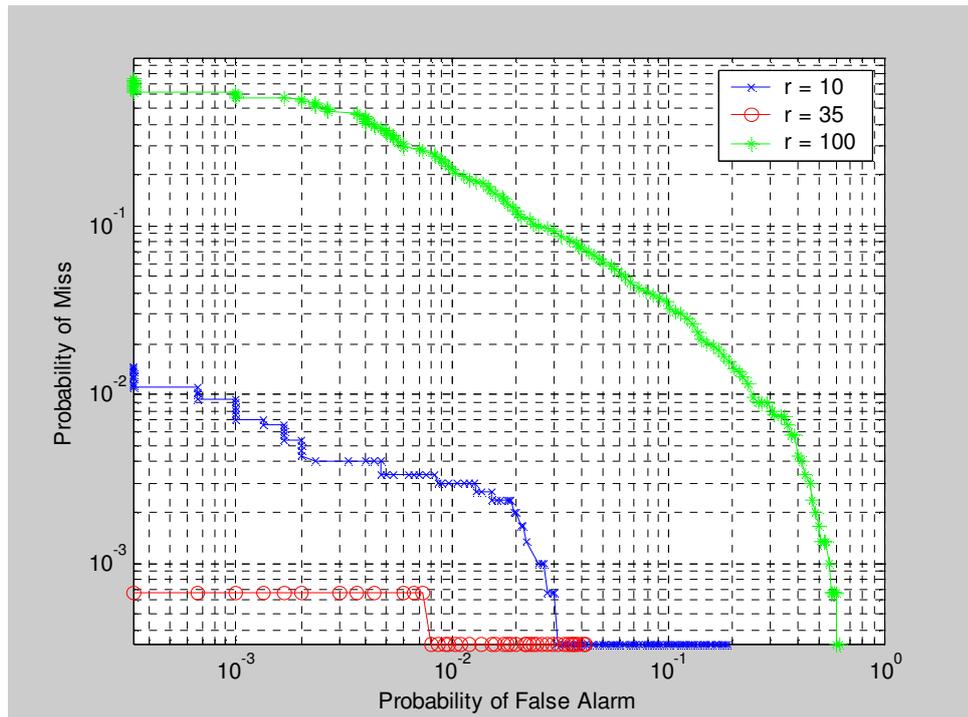


Figure 7.2. ROC curves for modified NMF with different 'r' values when PSNR=20db and no attack is implemented

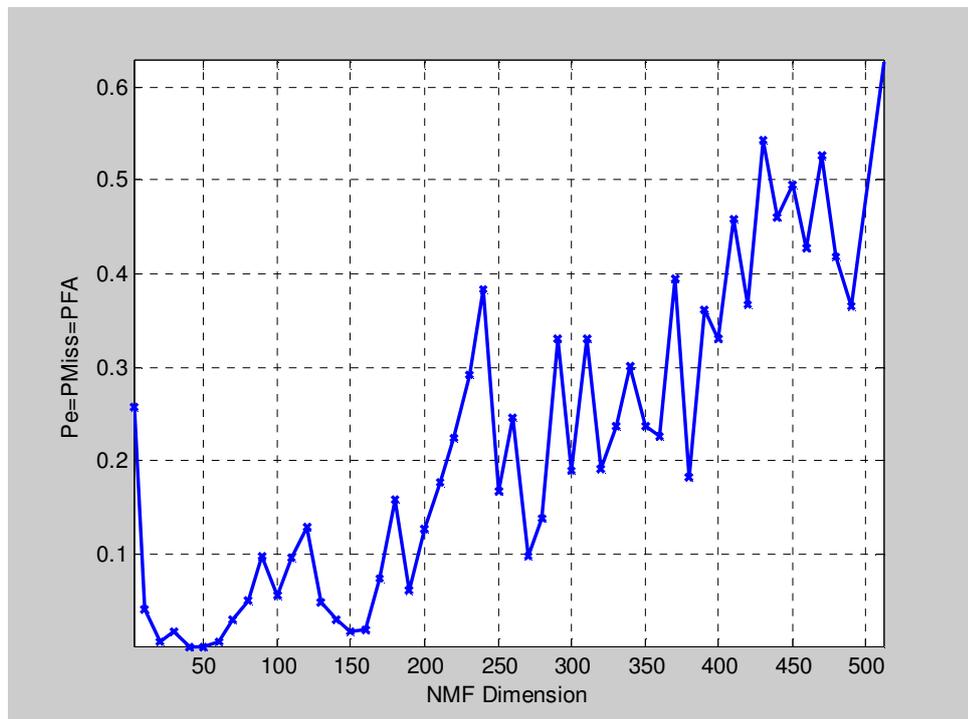


Figure 7.3. NMF dimension effect on the accuracy of the watermark verification measured in terms of probability of error

7.1.2. Watermark Power Related Modified NMF Simulations

The watermark power has a great influence of the performance of watermarking. The watermark power is measured relative to the cover image power in terms of PSNR using (7.2) in decibels. PSNR values between 20 and 30 db are acceptable values for watermark embedding. The simulations for modified NMF are conducted with three PSNR values 20, 25 and 30 db. It is observed from the simulations that the higher the watermark power, the higher the accuracy of the watermark verification. The simulations with NMF dimension of 35 is given in Figure 7.4.

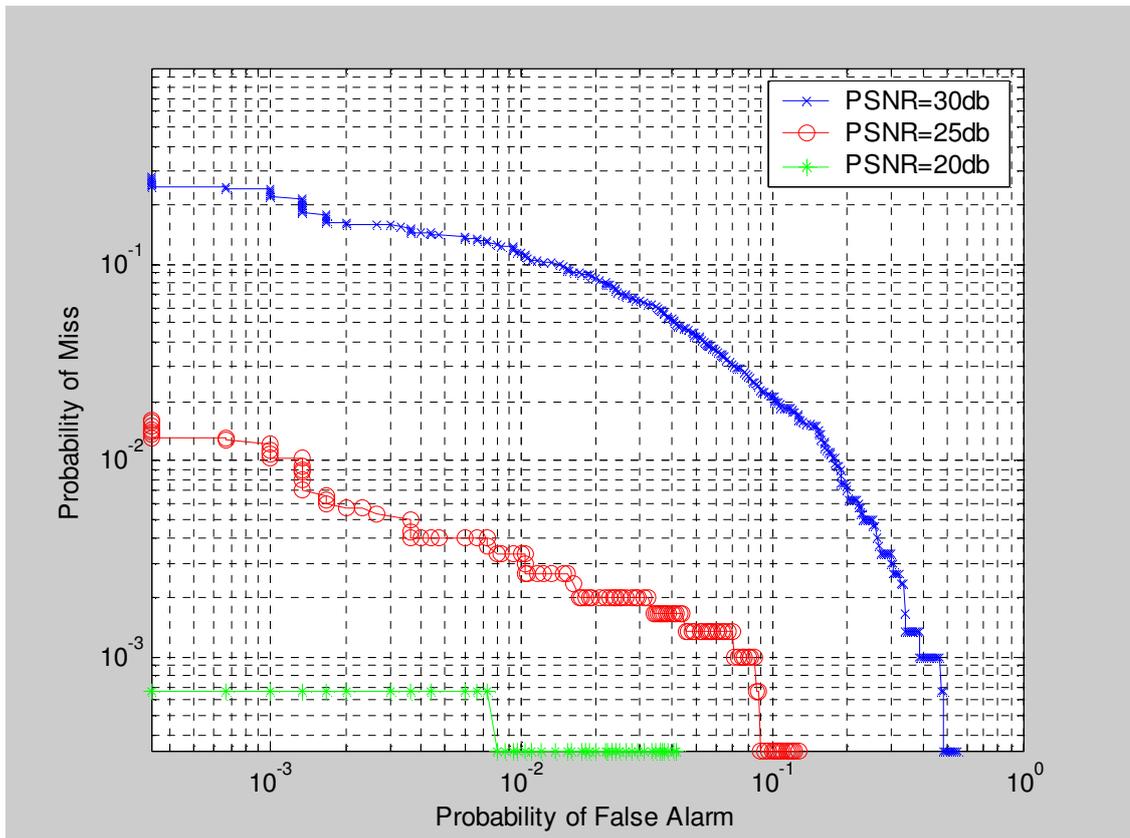


Figure 7.4. ROC curves for modified NMF with different watermark powers when NMF dimension=35 and no attack is implemented

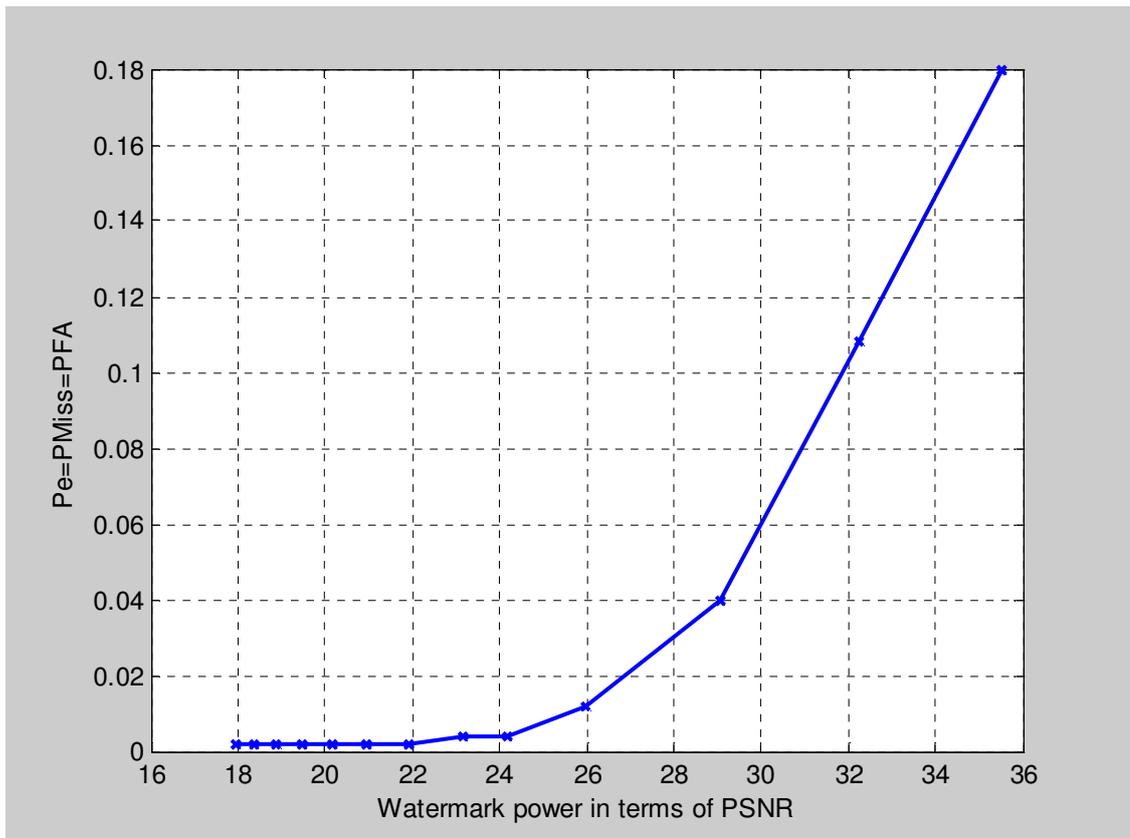


Figure 7.5. Watermark power effect on the accuracy of the watermark verification measured in terms of probability of error

7.1.3. AWGN Attack Related Modified NMF Simulations

Since the image passes through a channel, there might be external attacks or distortions applied to the image. Other than the watermark verification performance of the modified NMF algorithm without any external impacts, the robustness against various attacks should also be analyzed. AWGN attack is a common type of attack and is analyzed with various noise powers. Like watermark power, the noise power is measured in terms of PSNR (7.2). The noise power is calculated as the PSNR of the watermarked image and the attacked watermarked image.

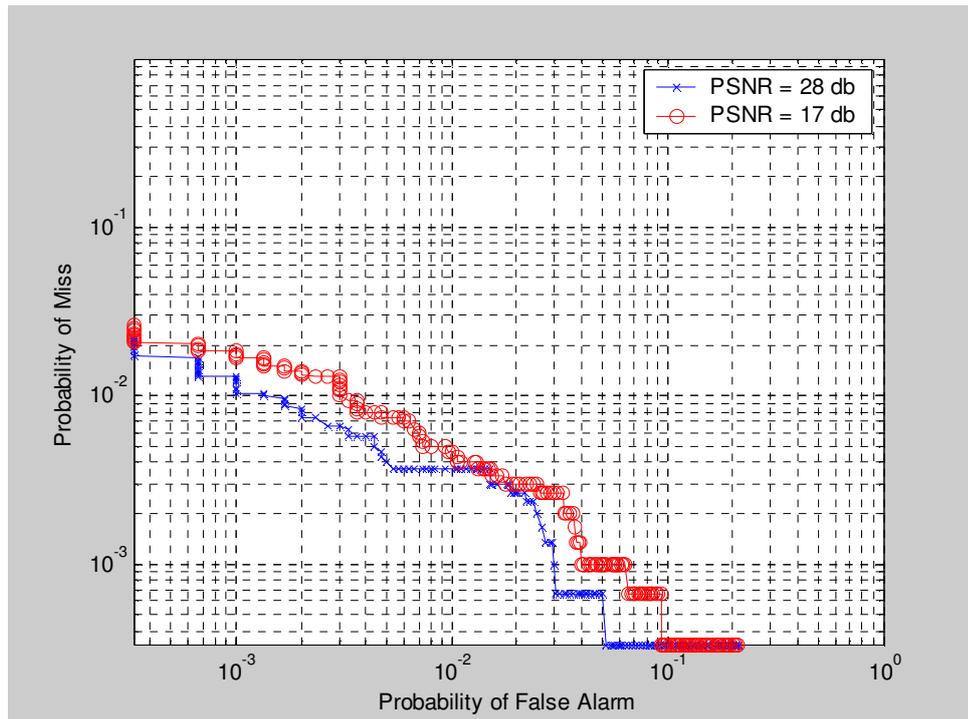


Figure 7.6. ROC curves for modified NMF with dimension=10 and watermark power=30 db is subject to AWGN attacks with different AWGN powers

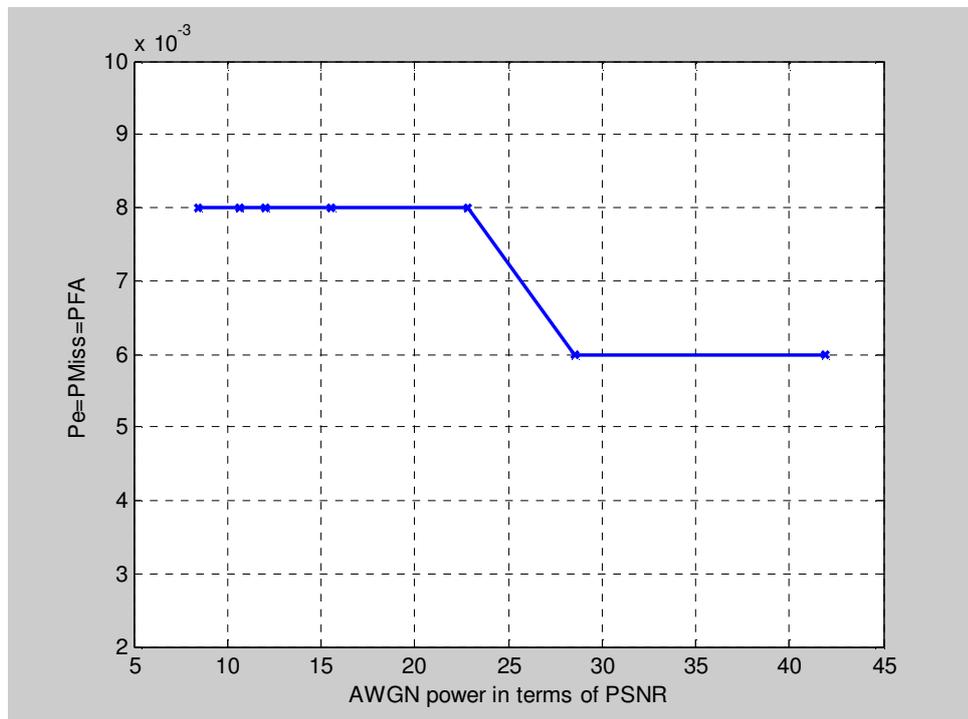


Figure 7.7. AWGN power effect on the accuracy of the watermark verification measured in terms of probability of error

As expected the increase in the power of the AWGN power, results in the inaccuracy of the watermark verification. The observation of the fact that the NMF dimension affects the watermark verification performance is also valid for the AWGN attacks as seen in

Figure 7.8. The watermark verification mechanism for AWGN attacks is most robust at the NMF dimension range of 30 – 50. Figure 7.9 also verifies the effect of the watermark power to the watermark verification performance. As explained in 7.1.2, the greater the watermark power, the higher the accuracy of the watermarking verification. This is also valid for the AWGN attacks.

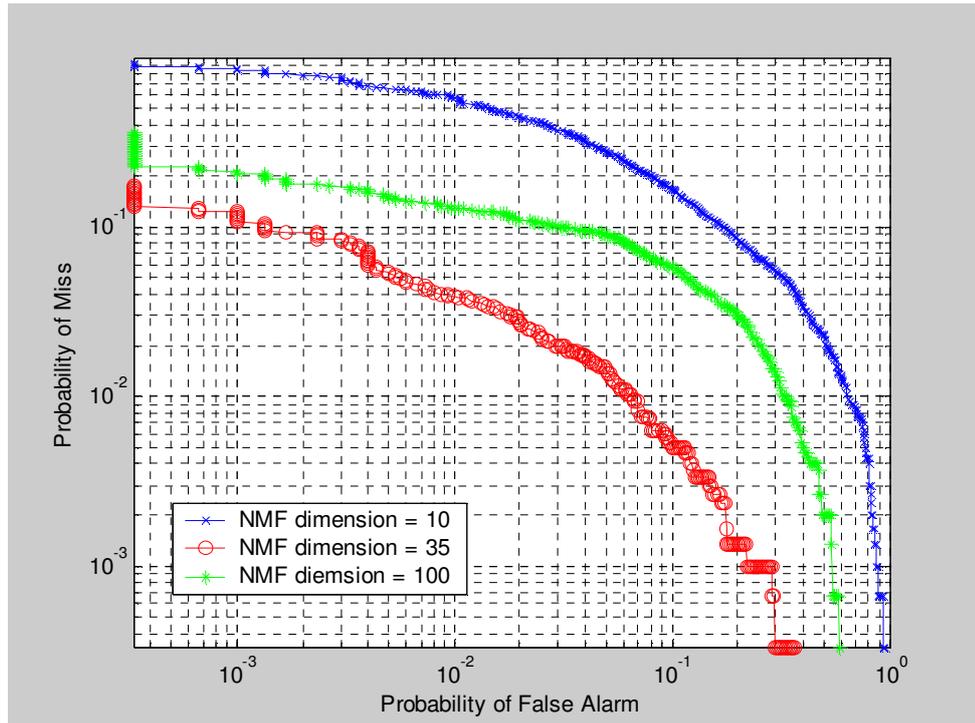


Figure 7.8. ROC curves for modified NMF with different dimensions and watermark power=30 db is subject to AWGN attacks with AWGN power = 18 db

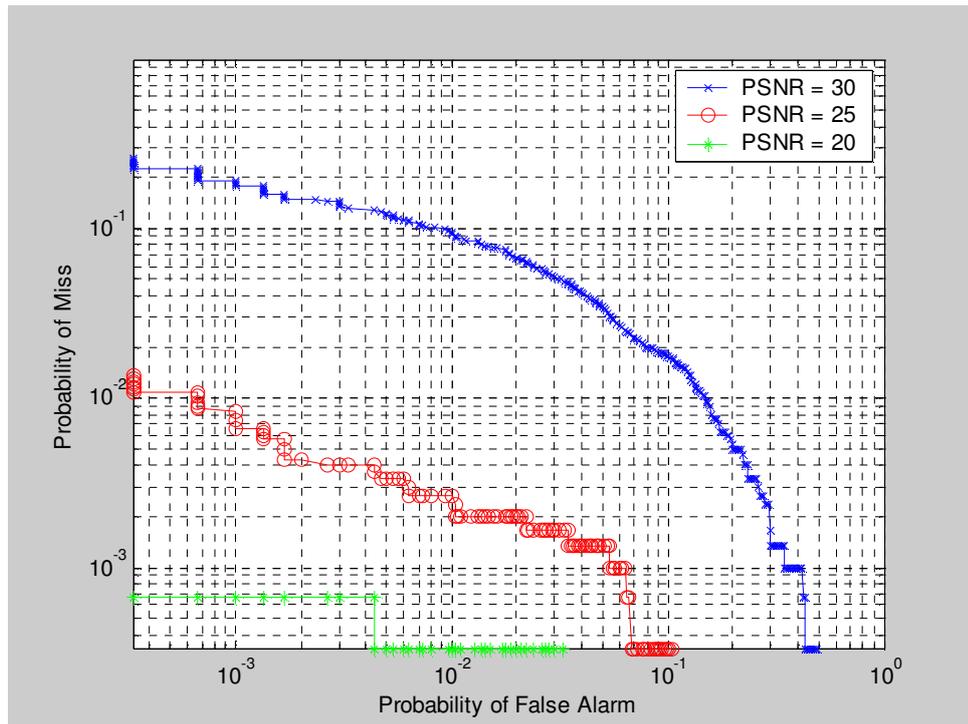


Figure 7.9. ROC curves for modified NMF with dimension=35 and different watermark powers is subject to AWGN attacks

7.1.4. JPEG Attack Related Modified NMF Simulations

The most general and expected attack is the additive noise attack that examined in 7.1.4. Other than AWGN, the watermarked image might be subjected to compression attacks such as JPEG compression. The JPEG compression is simulated with `imwrite` and `imread` functions of Matlab. The amount of the compression can be determined via 'quality' parameter.

Although the JPEG compression can be measured with the quality parameter of the `imwrite` function, the distortion is also measured in terms of PSNR of the watermarked image and compressed watermarked image.

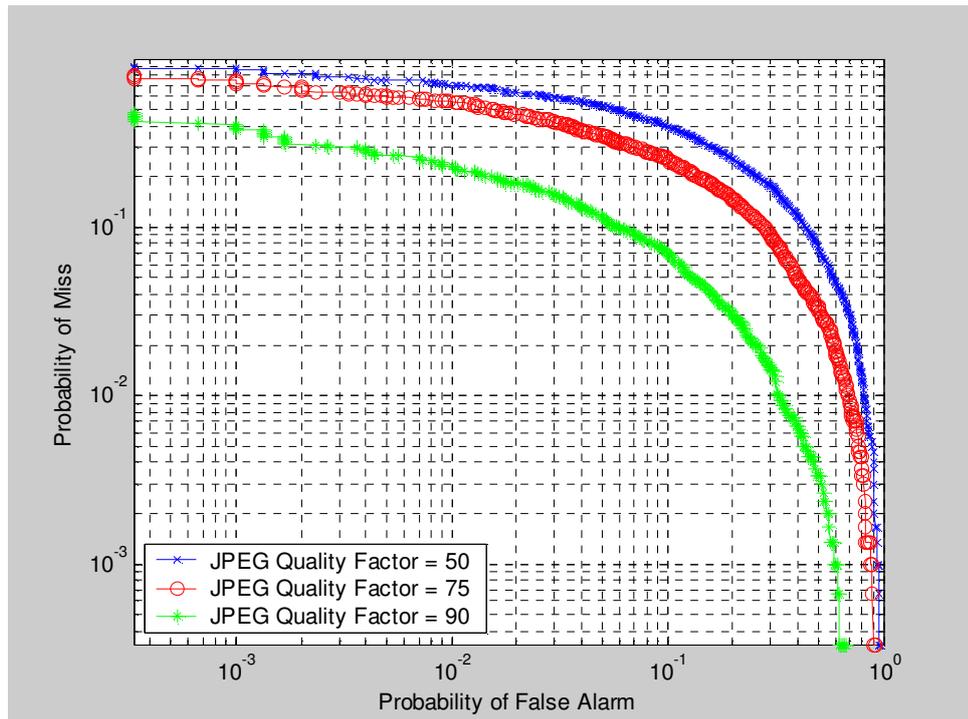


Figure 7.10. ROC curves for modified NMF with dimension=35 and watermark power=25 db is subject to JPEG compression attacks with different quality factors

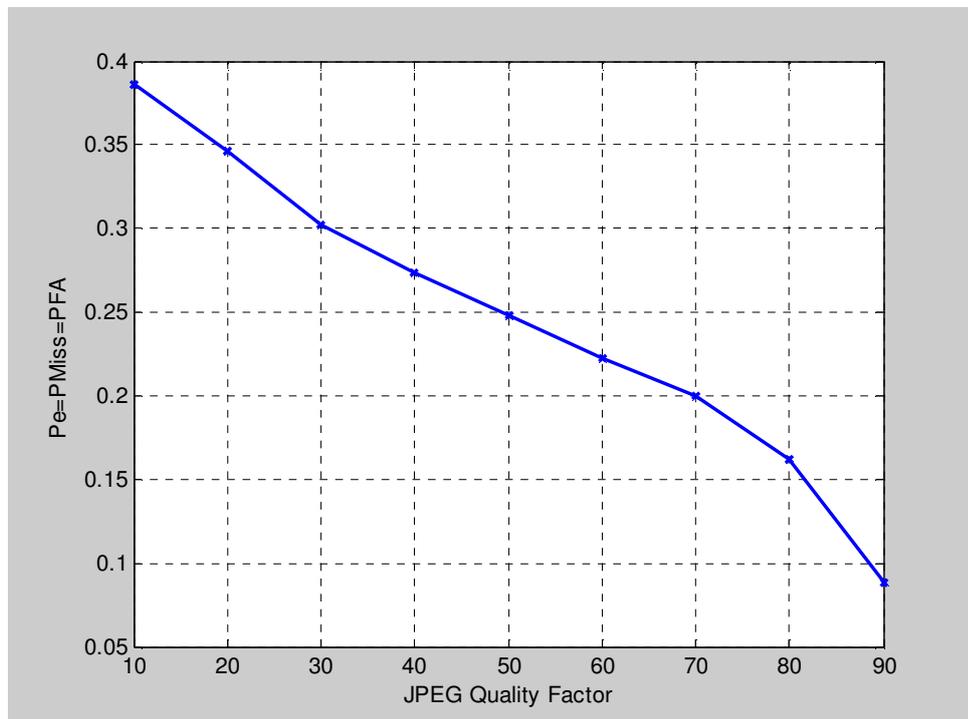


Figure 7.11. JPEG quality effect on the accuracy of the watermark verification measured in terms of probability of error

The JPEG compression quality factor provides information about the distortion of the watermarked images. However the PSNR values corresponding to these JPEG

compression quality factors are also derived. PSNR values of 25 db, 39 db, 43 db correspond to the JPEG compression factors 50, 75 and 90 respectively.

According to the simulation results it can be identified that for the JPEG compressions that results in more image distortion, have more negative effect on the watermark verification performance.

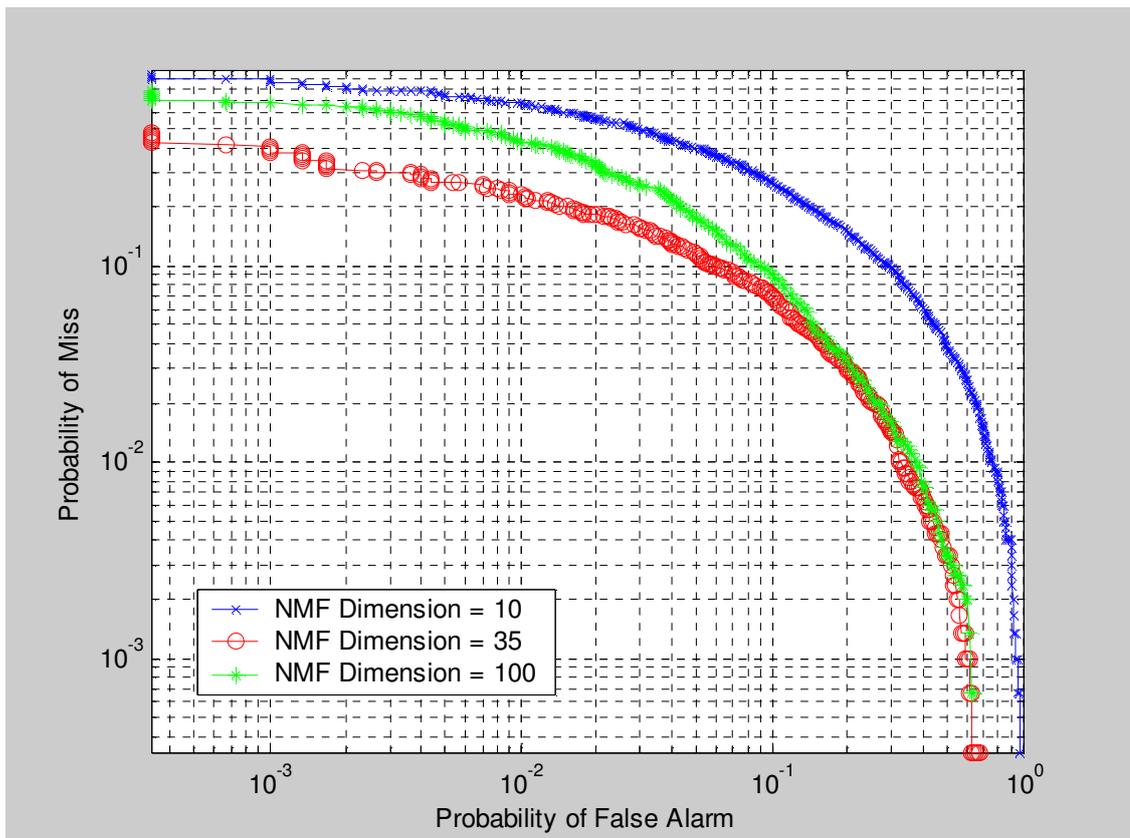


Figure 7.12. ROC curves for modified NMF with different NMF dimensions and watermark power=25 db is subject to JPEG compression attacks with quality factor = 90

Figure 7.12 provides the same result as the NMF dimension effect on the watermark verification performance. It is observed that there exists an optimum NMF dimension range about 30 – 50. The values higher or lower than these values have more in accuracy in the verification. Figure 7.13 expresses the watermark power effect on the JPEG compression attacks. As expected the increase in watermark power has a positive effect on the watermark verification accuracy.

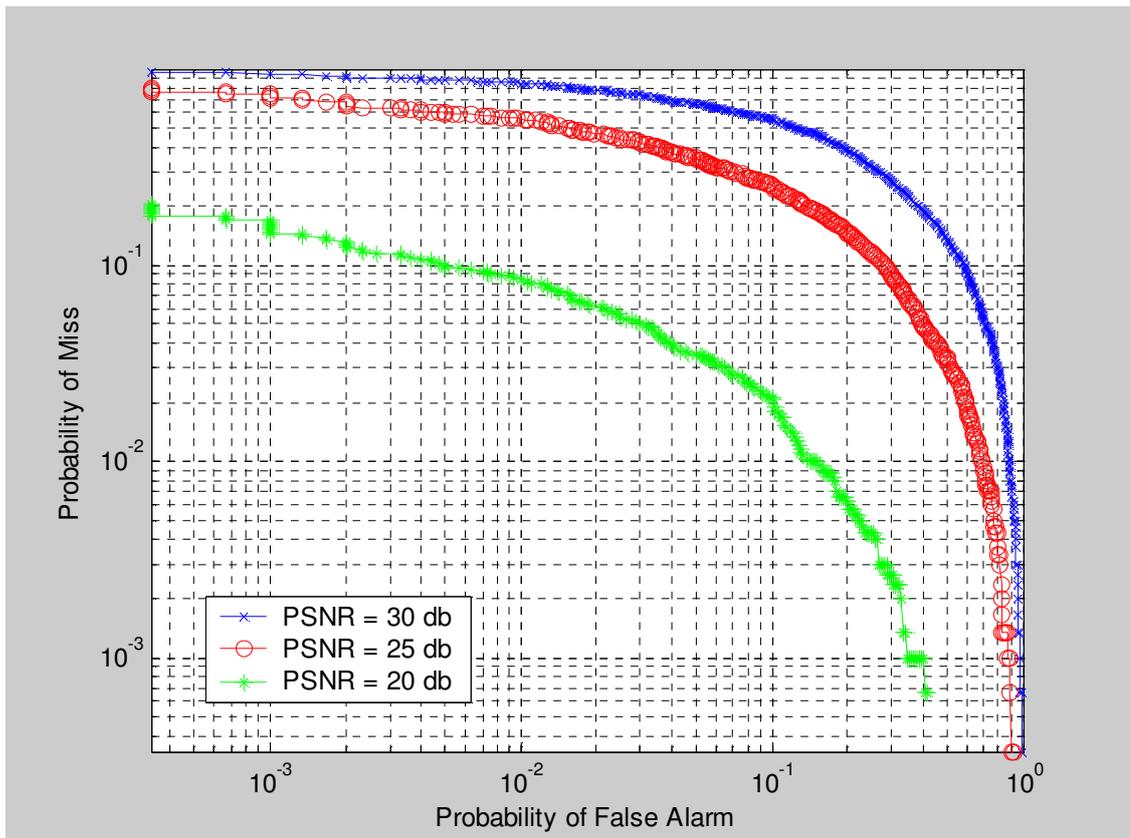


Figure 7.13. ROC curves for modified NMF with NMF dimension=35 and different watermark powers is subject to JPEG compression attacks with quality factor = 75

7.1.5. Rotation Attack Related Modified NMF Simulations

When image processing is considered, the geometric attacks are the most common attacks applied to images. In the simulations rotation and scaling attacks are taken into account. Since the geometric attacks results in more perceptual distortion compared to JPEG compression or AWGN attacks, the parameters for the geometric attacks are kept in the lower measures. To simulate the image rotation the `imrotate` function of Matlab is used with bicubic and crop parameters so that the size of the image is kept constant during rotation attack simulations.

The distortion for the image rotation attack is measured with the PSNR value of the watermarked image and the rotated watermarked image. The simulation results for rotation attacks are given in Figure 7.14.

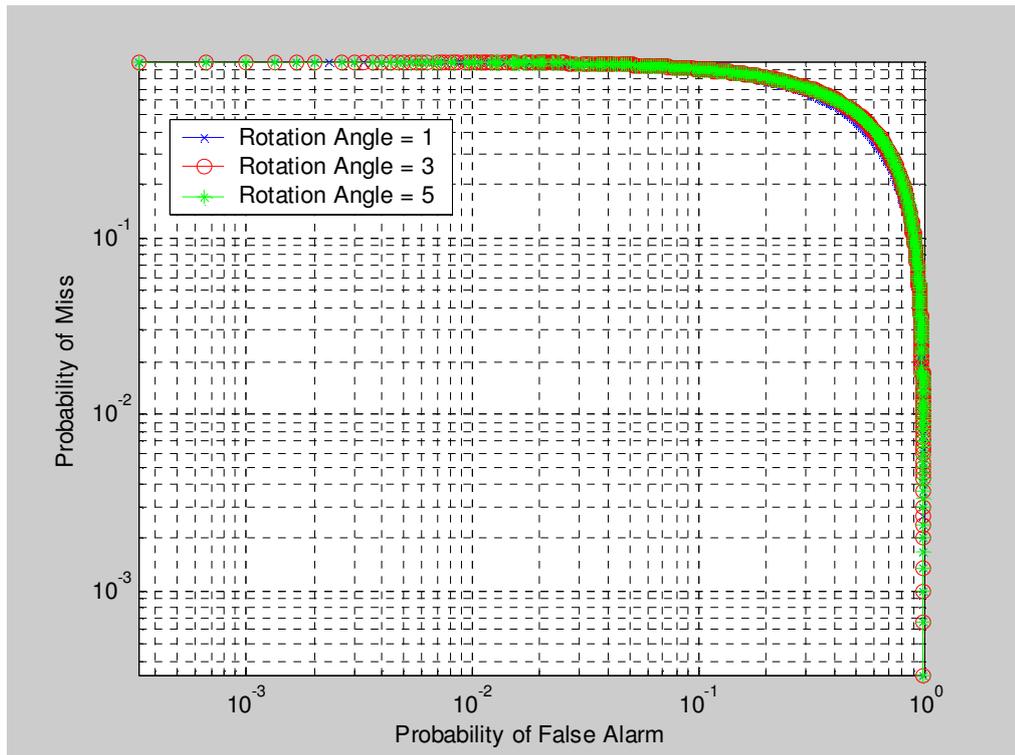


Figure 7.14. ROC curves for modified NMF with dimension=35 and watermark power=25 db is subject to rotation attacks with different rotation angles

It can be clearly observed that watermark verification using modified NMF algorithm is not resilient to rotation attacks. Even if the rotation angles are kept small to minimize the distortion of the image, the performance is very low. Since the watermark verification with modified NMF is not robust to rotation attack, the variations in the watermark power or the NMF dimension do not have a greater effect as seen in Figure 7.16 and 7.17. For the rotation attack simulations, the disturbances of the watermarked images are 15 db, 13 db and 12 db respectively for rotation angle of 1, 3 and 5 degrees.

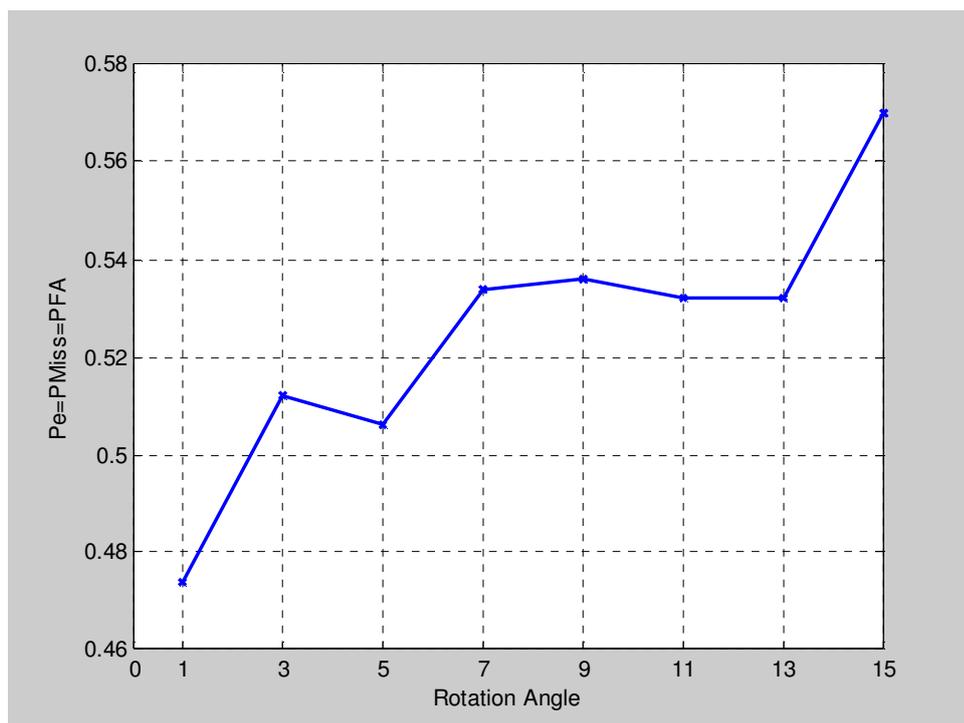


Figure 7.15. Rotation angle effect on the accuracy of the watermark verification measured in terms of probability of error

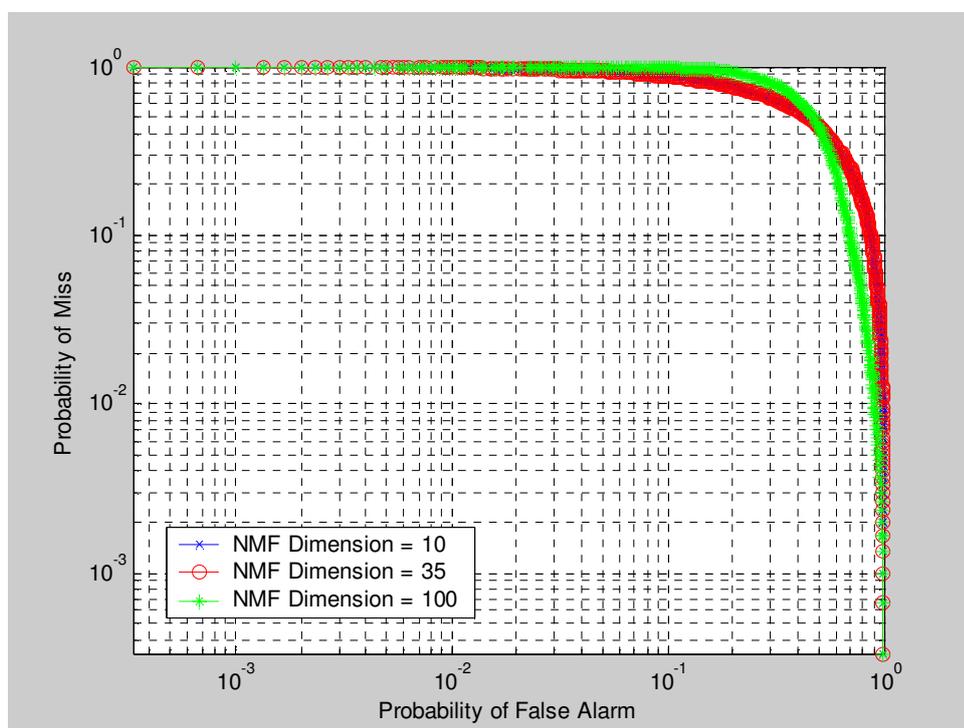


Figure 7.16. ROC curves for modified NMF with different dimension and watermark power=20 db is subject to rotation attacks with rotation angle=1

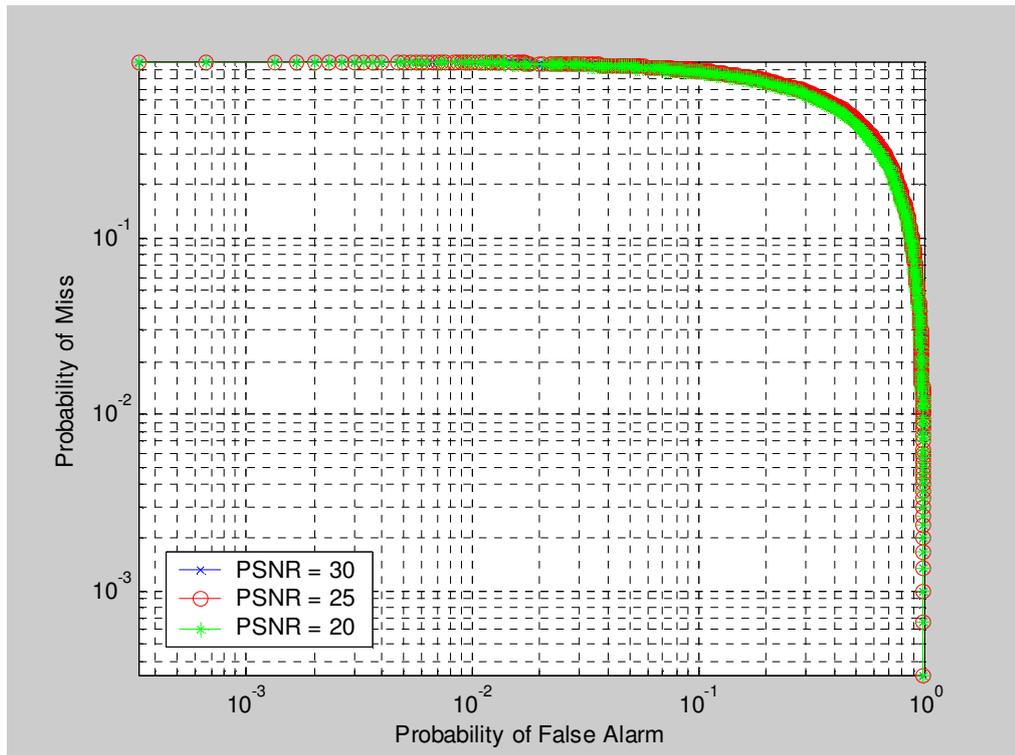


Figure 7.17. ROC curves for modified NMF with dimension=35 and different watermark powers is subject to rotation attacks with rotation angle=1

7.1.6. Scaling Attack Related Modified NMF Simulations

Another geometric attack applied to the watermarked image during the simulations is the scaling attack. The difference for the scaling simulations is the fact that the distortion cannot be measured as PSNR since the size of the watermarked image and the scaled watermarked image are not the same.

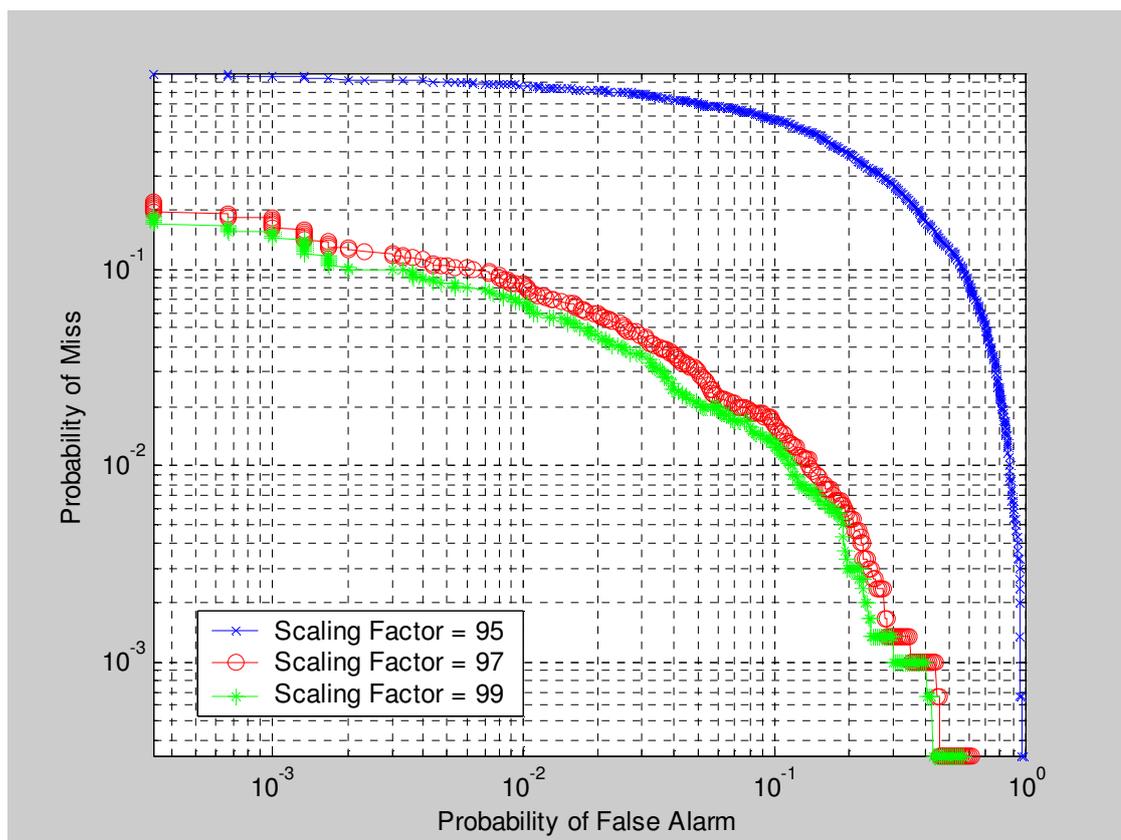


Figure 7.18. ROC curves for modified NMF with dimension=35 and watermark power=25 db is subject to scaling attacks with different scaling factors

After the scaling attack is applied to the watermarked image, the image is rescaled to 512x512 since all the images are normalized to 512x512 no matter what the original sizes are. For simulating the scaling imresize function of Matlab with bicubic parameter is used. The scaling factor is the scaling per cent of the image, that is if the scaling factor is 97 per cent then the image is scaled to 97 per cent to its original size.

Figure 7.18 shows the fact that similar to rotation attack; the watermark verification with modified NMF algorithm is not resilient to scaling attack. It can tolerate only minor attacks. It can be observed from Figure 7.20 and Figure 7.21 that the performance of the watermark verification with modified NMF mechanism under scaling attack depends on the watermark power and NMF dimension. However it should be noted that this is valid only for minor scaling attacks. For strong attacks the performance of the mechanism decreases dramatically as for rotation attacks.

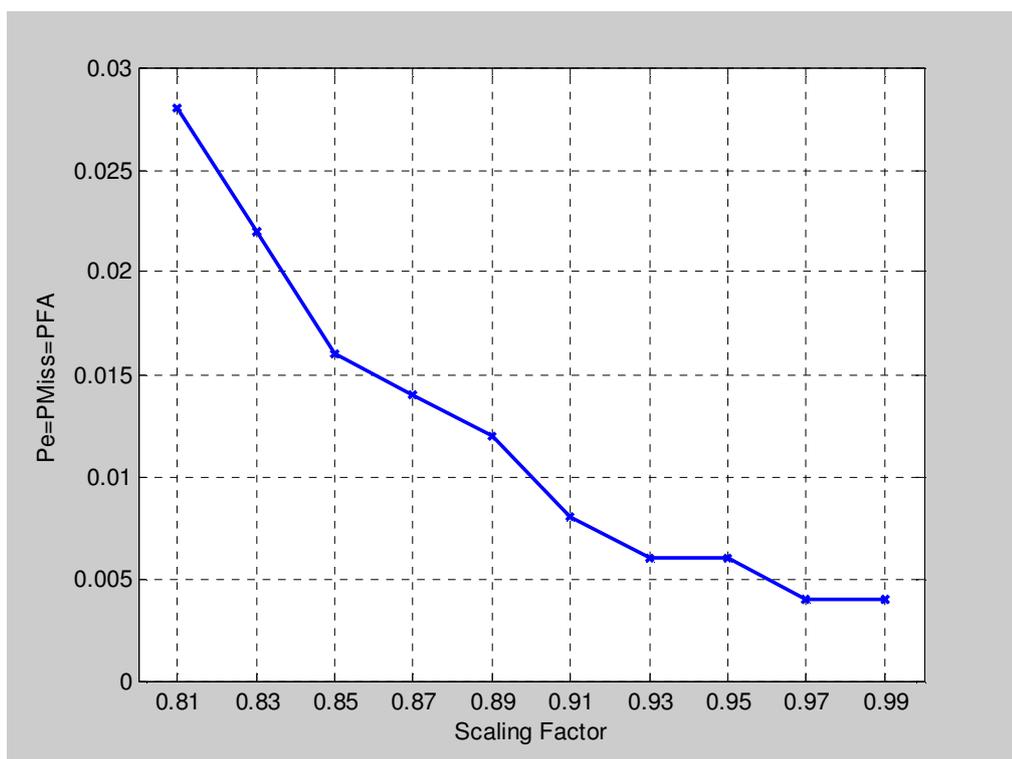


Figure 7.19. Scaling factor effect on the accuracy of the watermark verification measured in terms of probability of error

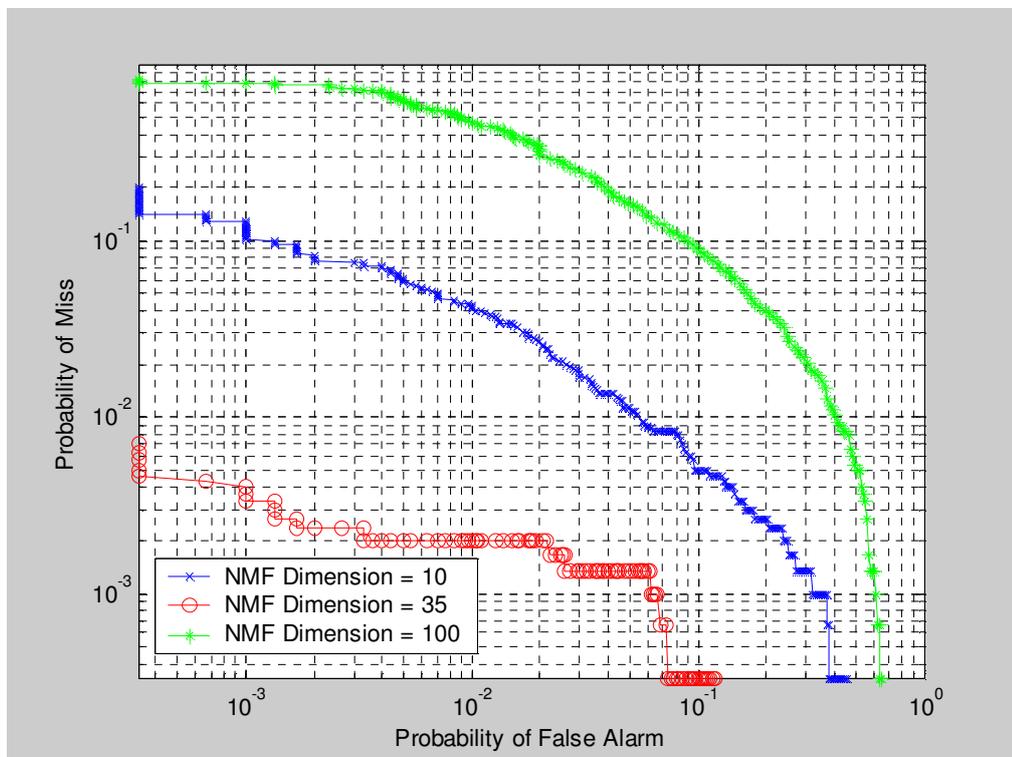


Figure 7.20. ROC curves for modified NMF with different dimensions and watermark power=20 db is subject to scaling attack with scaling factors 0.99

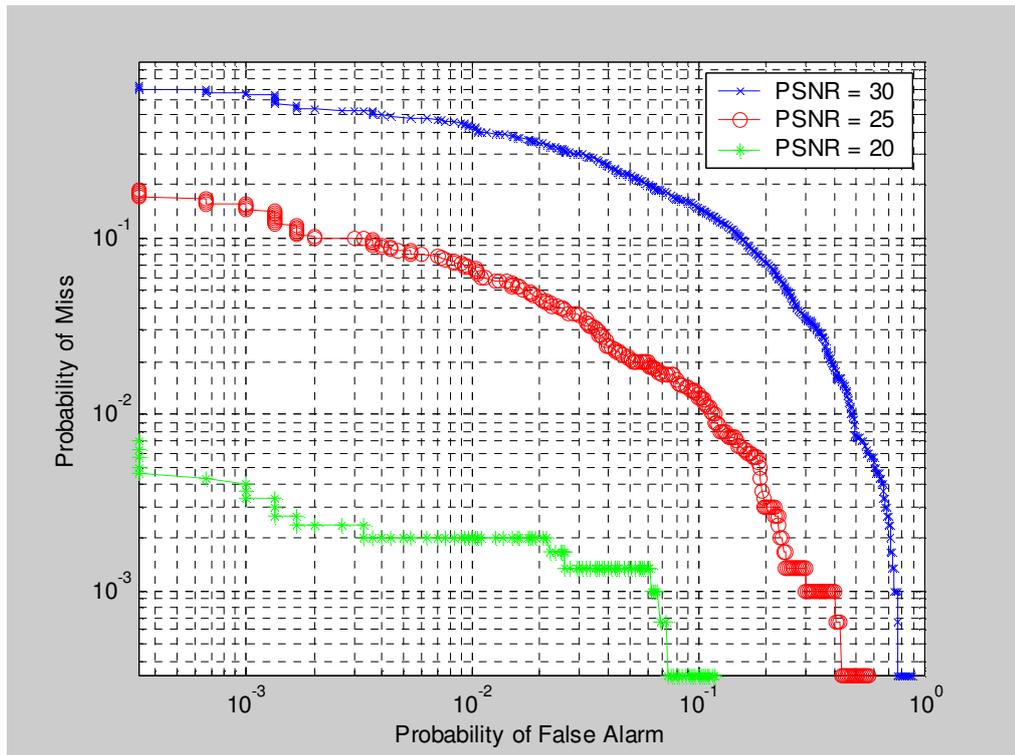


Figure 7.21. ROC curves for modified NMF with dimension=35 and different watermark powers is subject to scaling attack with scaling factors 0.99

7.2. Simulations for Comparison of Watermark Verification Using Multiplicative, NMF-SVD and Modified NMF

The performance of the proposed watermarking algorithm based on modified NMF is examined in section 7.1. In order to make a complete analysis the proposed method, the performance of this method should be compared to other methods like watermarking with multiplicative NMF which is explained in section four and watermarking with NMF-SVD which is explained in section five.

The simulation bed is the same as section 7.1. The image is watermarked using one of the three algorithms and passes through a channel.

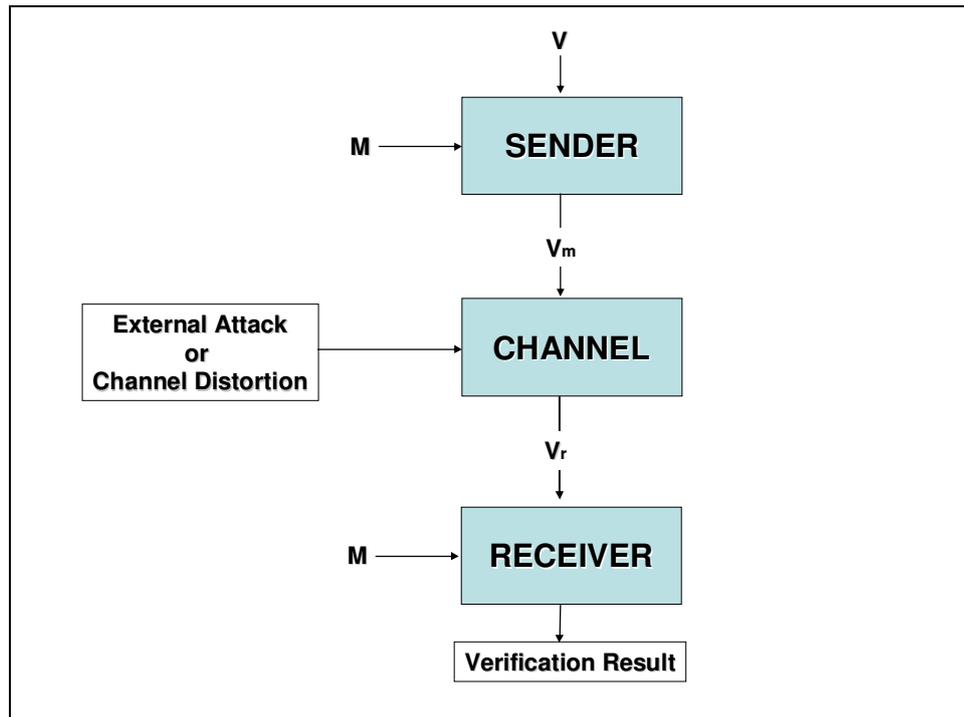


Figure 7.22. Simulation diagram for algorithms other than modified NMF

The difference is that since multiplicative NMF and SVD-NMF algorithms do not have a fixed W matrix, it should not be given as an input parameter for these methods. As explained in sections 4.1 and 5.1 the watermark embedding requires calculation of NMF, therefore these two algorithms take more time than modified NMF algorithm. The simulations consist of basic embedding and verification method without any attacks and the cases where the following attacks are applied to the watermarked image:

- Additive White Gaussian Noise (AWGN)
- JPEG Compression
- Rotation
- Scaling

It is verified that modified NMF algorithm operates at its best performance when the NMF dimension is about 35. As a result of this observation, the comparison simulations are performed with NMF dimension of 35 for convenience.

7.2.1. Performance Relations without Any Attack

The performance criteria of modified NMF are studied in sections 7.1.1 and 7.1.2. According to the simulations the performance of modified NMF based algorithm is affected by the NMF dimension and the watermark power. In these simulations the performances of the modified NMF, multiplicative NMF and NMF-SVD algorithms are compared under same circumstances like same initial conditions. The maximum number of iterations and thresholds are the same for NMF algorithms.

The simulation results obtained from Figures 7.23, 7.24 and 7.25 points out that the watermark verification algorithm based on modified NMF has a better performance than the other two methods. NMF-SVD method has a low performance compared to other two algorithms. Watermark verification algorithm based on multiplicative NMF has a better performance than the NMF-SVD but still less efficient than the watermarking algorithm based on modified NMF.

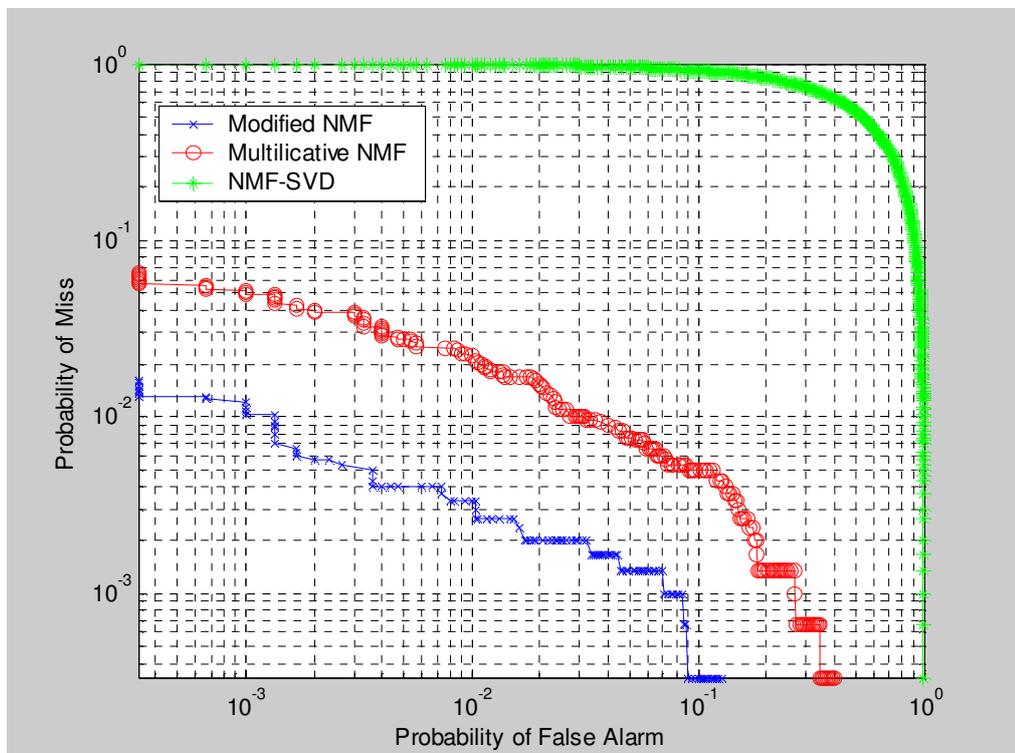


Figure 7.23. ROC curves for different methods when NMF dimension=35 and watermark power=25 db

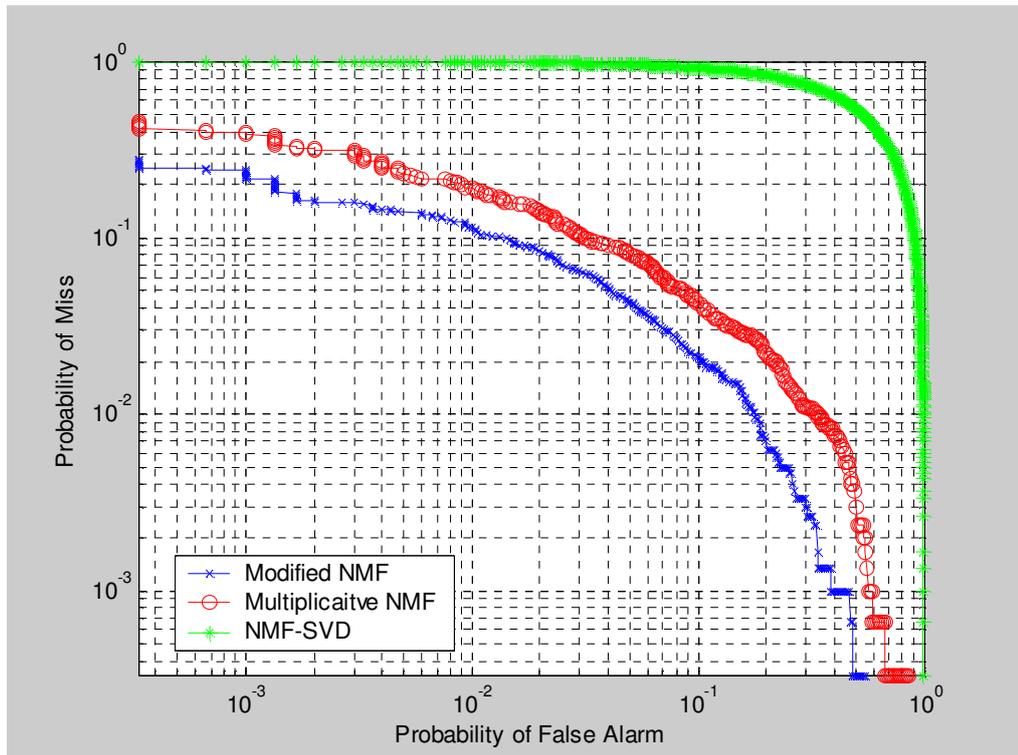


Figure 7.24. ROC curves for different methods when NMF dimension=35 and watermark power=30 db

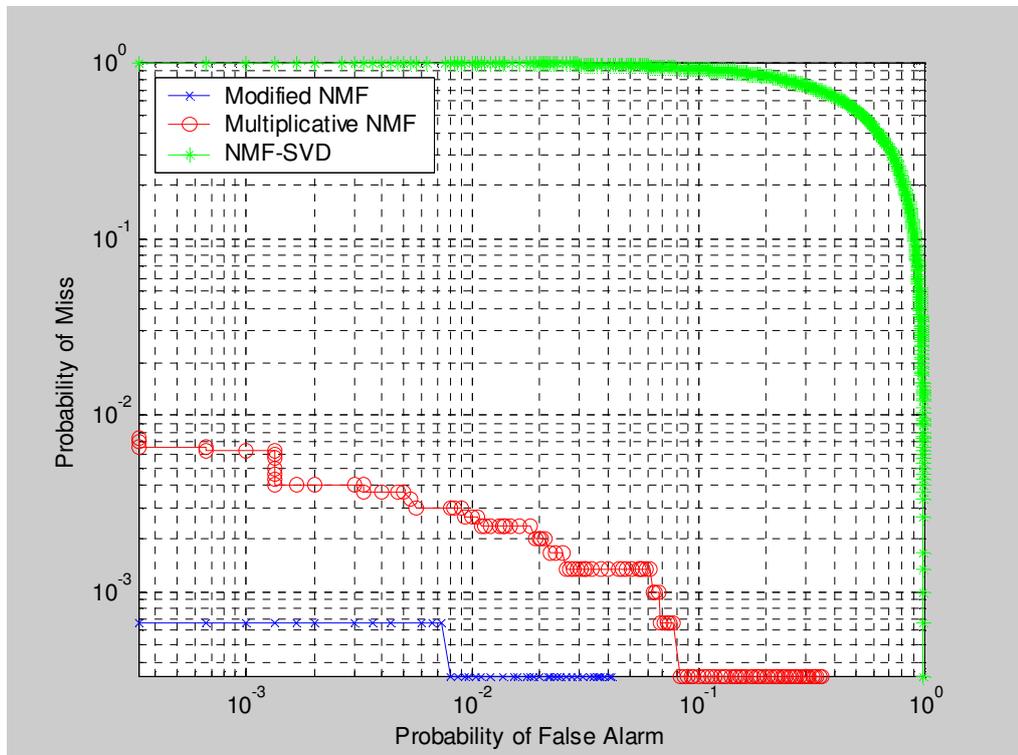


Figure 7.25. ROC curves for different methods when NMF dimension=35 and watermark power=20 db

7.2.2. AWGN Attack Related Simulations

The performance of watermark verification with modified NMF algorithm is analyzed in section 7.1.3. The effects of watermark power and the NMF dimension are also analyzed separately. The effect of the AWGN attack on the performance of other two algorithms is also examined. The same watermark with different powers is used for all the three algorithms with same initial conditions.

Similar to the simulations without any attack, modified NMF based watermark verification algorithm has the most efficiency in verifying the watermark among three algorithms. It is observed from the Figures 7.26, 7.27 and 7.28 that as the watermark power decreases the performance difference between the multiplicative NMF and modified NMF decreases.

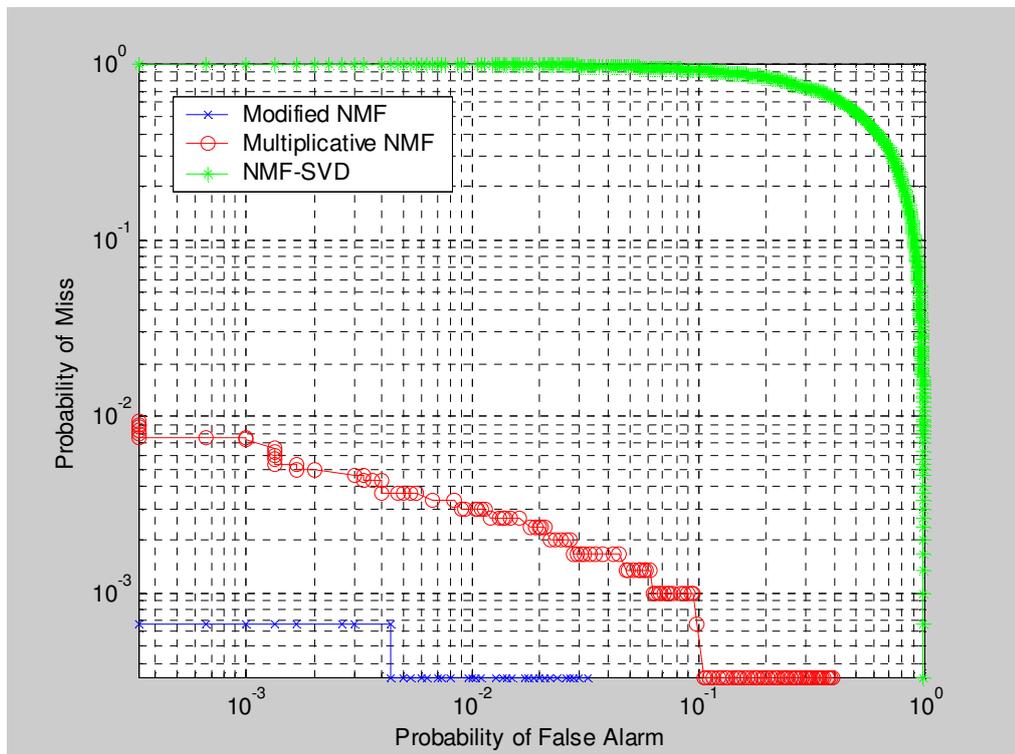


Figure 7.26. ROC curves for different methods when NMF dimension=35 and watermark power=20 db and image is subject to AWGN attack

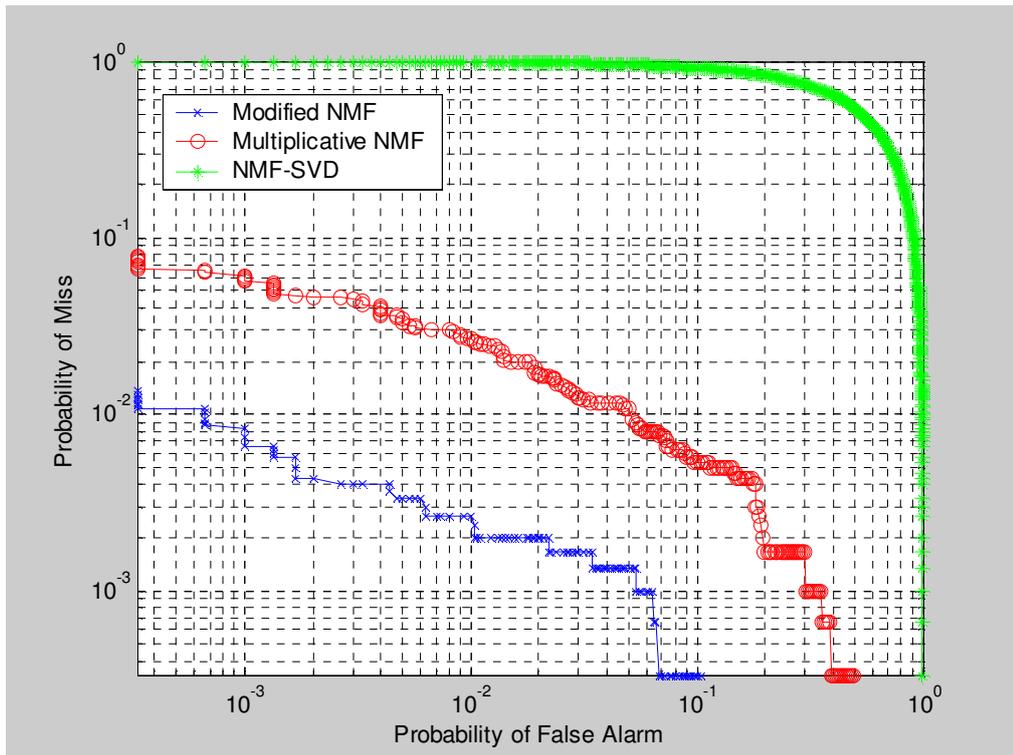


Figure 7.27. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to AWGN attack

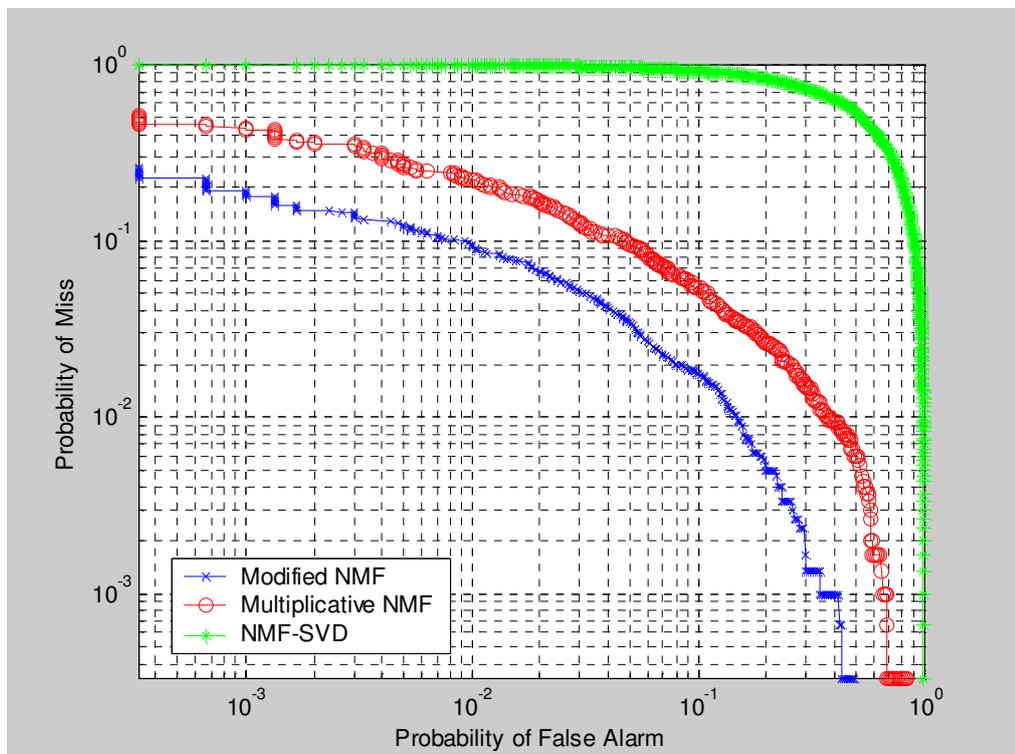


Figure 7.28. ROC curves for different methods when NMF dimension=35 and watermark power=30 db and image is subject to AWGN attack

7.2.3. JPEG Compression Attack Related Simulations

In section 7.1.4, JPEG compression attack is applied to modified NMF based watermarking algorithm and the results are analyzed. The same JPEG compression attacks are applied to multiplicative NMF and NMF-SVD based watermarking verification algorithms.

In the JPEG compression attack simulations, contrary to AWGN attack simulation results, multiplicative NMF based watermark verification algorithm has a better performance than modified NMF based watermark verification algorithm. However it should be noted that all the algorithms have similar performances with small variances.

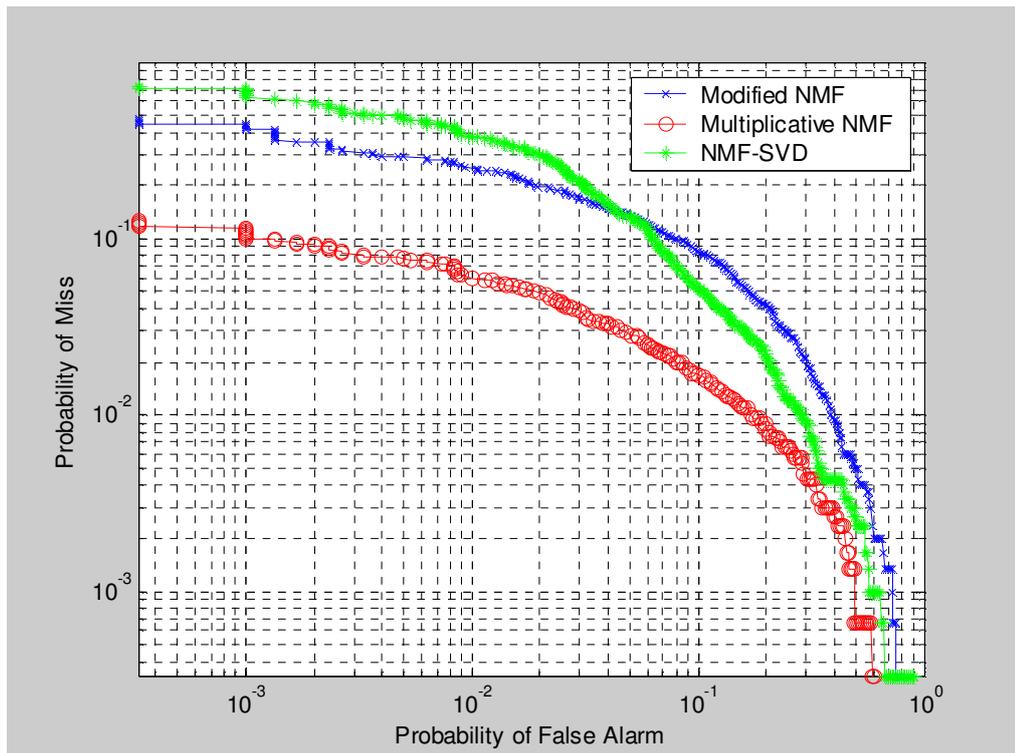


Figure 7.29. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to JPEG attack of quality=50

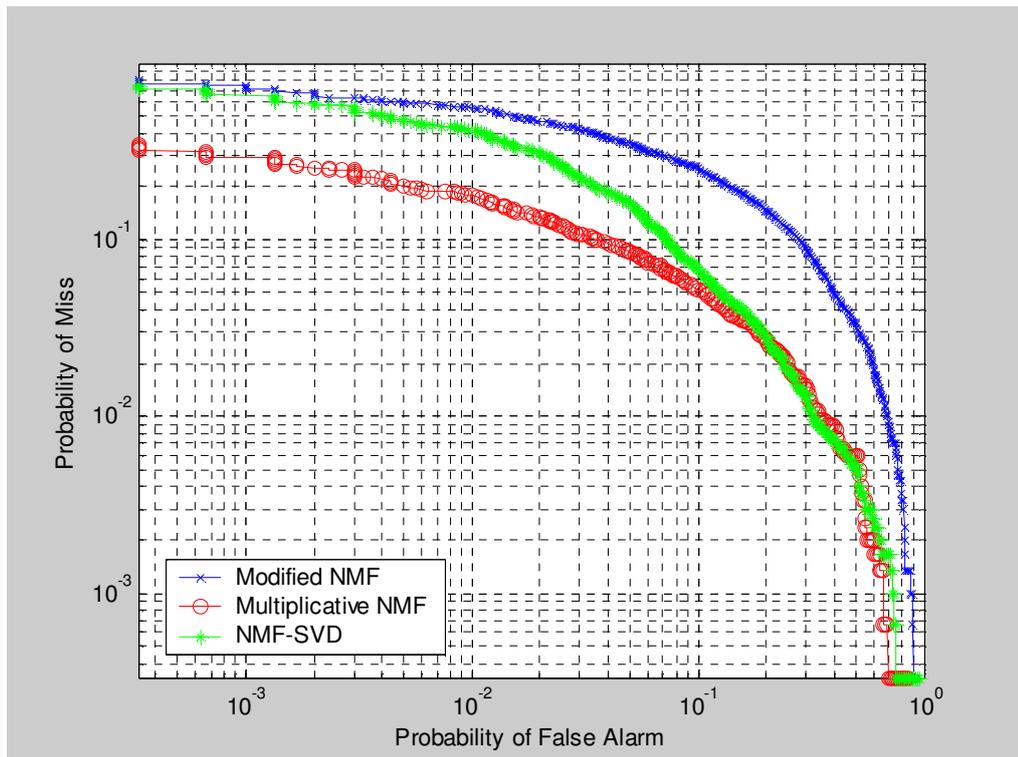


Figure 7.30. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to JPEG attack of quality=75

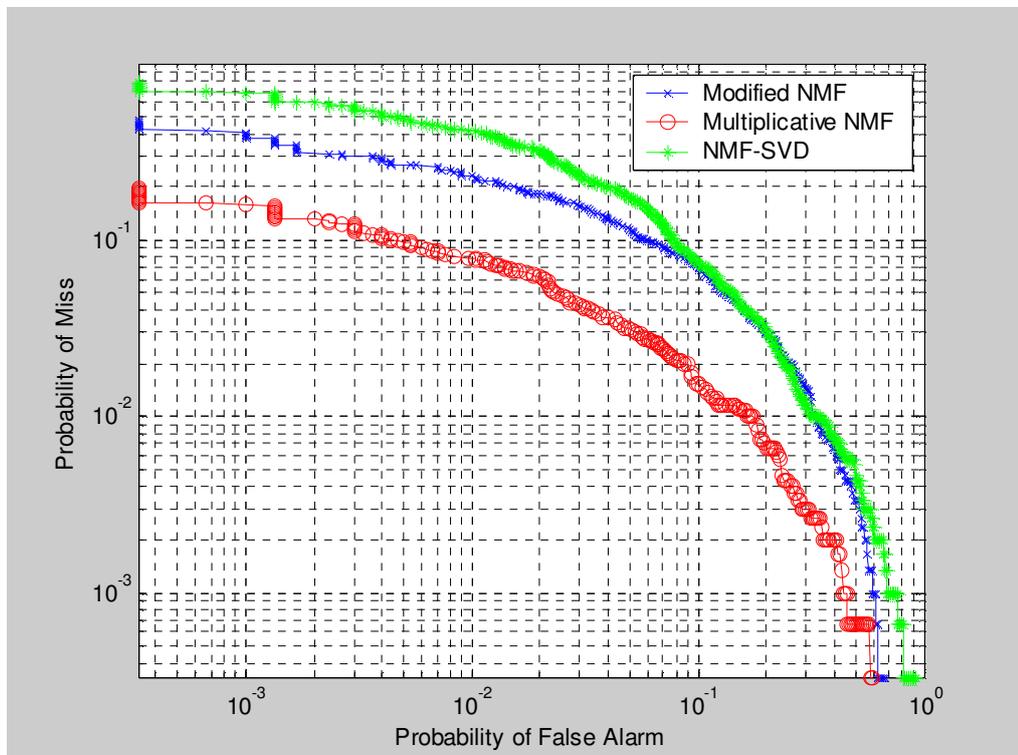


Figure 7.31. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to JPEG attack of quality=90

7.2.4. Rotation Attack Related Simulations

Rotation attack is one of the geometric attacks studied in this thesis. In section 7.1.5 the performance of modified NMF based watermarking verification algorithm is studied and concluded that it does not have a good performance measures under rotation attacks even under small angles of rotation. Due to this fact the simulations for other algorithms are also performed with small angle of rotations. The simulations are also performed with different watermarks.

As expected, like modified NMF based watermarking verification algorithm the other two watermark verification algorithms are not resilient to rotation attacks even in small degrees. Figures 7.32, 7.33 and 7.34 shows that, all three algorithms have bad performance even under 1 degree of rotation.

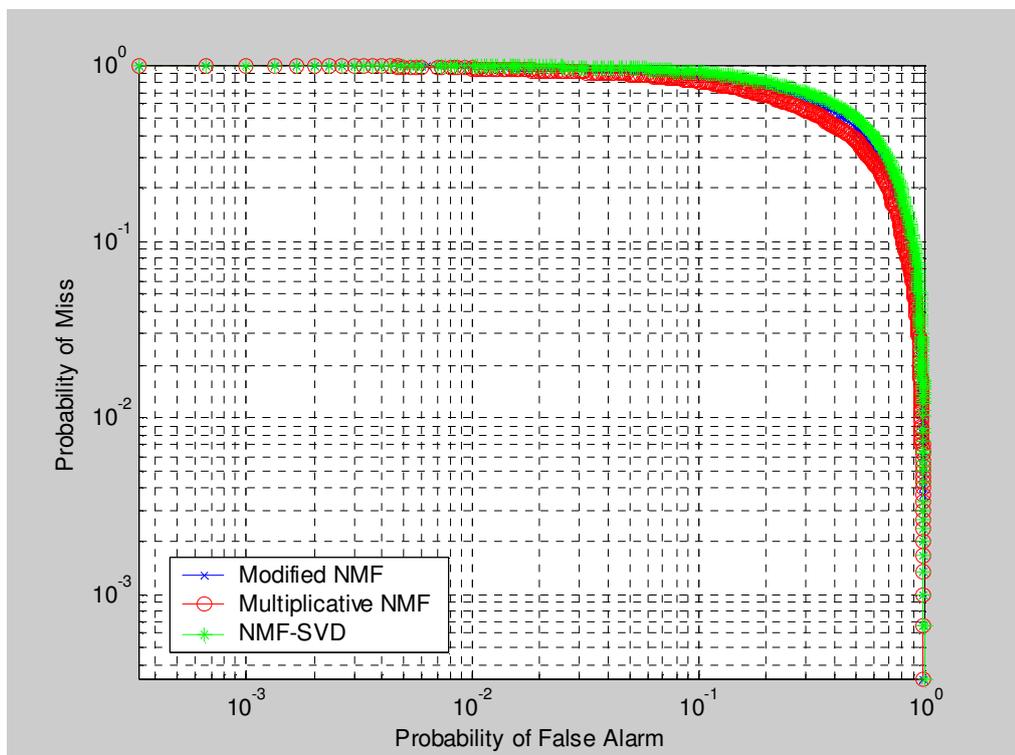


Figure 7.32. ROC curves for different methods when NMF dimension=35 and watermark power=20 db and image is subject to rotation attack of 1 degree

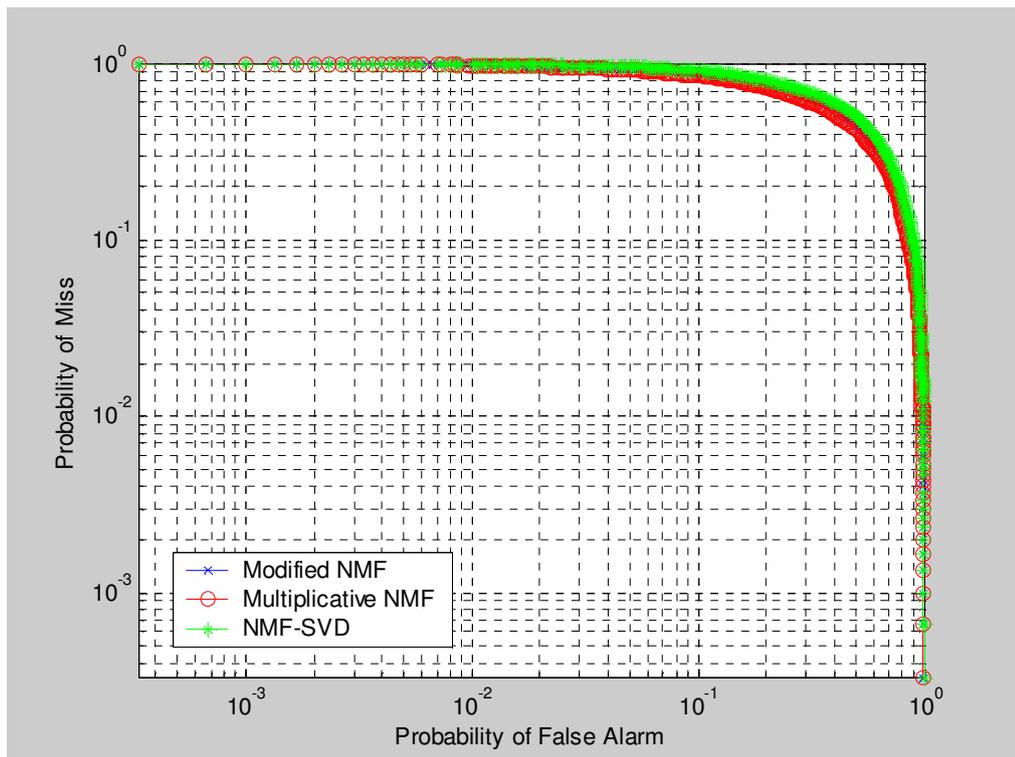


Figure 7.33. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to rotation attack of 1 degree

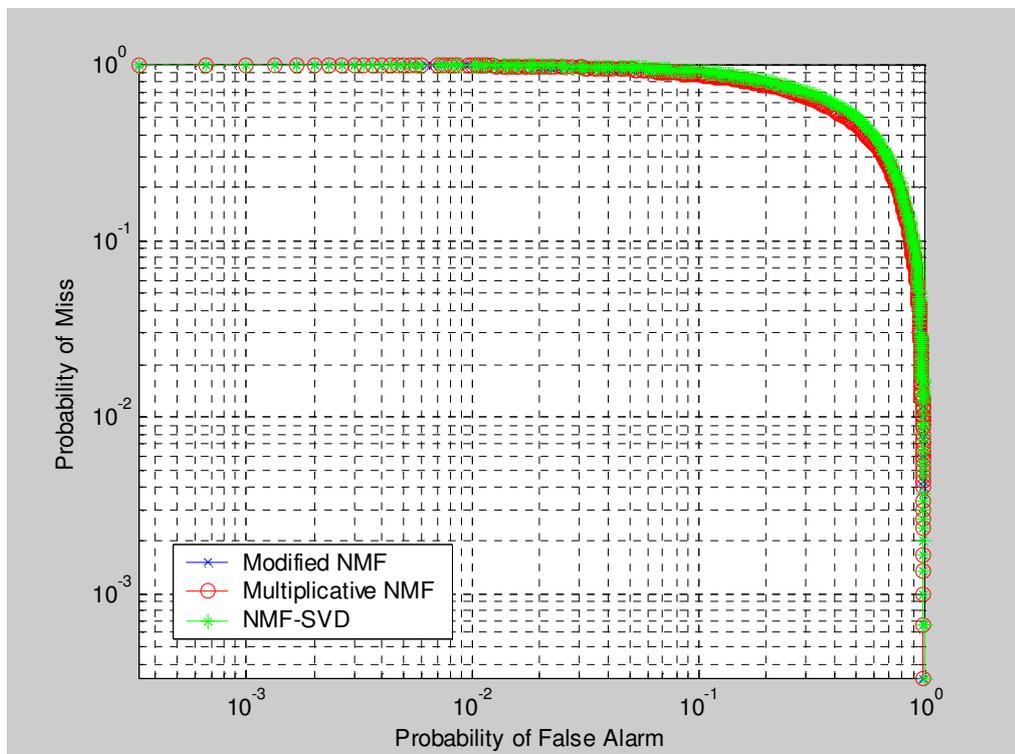


Figure 7.34. ROC curves for different methods when NMF dimension=35 and watermark power=30 db and image is subject to rotation attack of 1 degree

7.2.5. Scaling Attack Related Simulations

Another geometric attack is the scaling attack that simulated in the scope of this thesis. It is obtained from section 7.1.6 that watermarking verification algorithm based on modified NMF has dependency on scaling factor in terms of verification accuracy. For larger deviations the performance of the algorithm decreases dramatically.

The simulations of all three algorithms show that watermark verification algorithm based on modified NMF is the most accurate one among others. However it should be noted that this is valid only for small variations in the size. As the distortion due to scaling increases all three algorithms have a dramatic decrease in their performances. In addition from figures 7.35, 7.36 and 7.37 it is obtained that as the watermark power decreases all three algorithms affected in a negative manner.

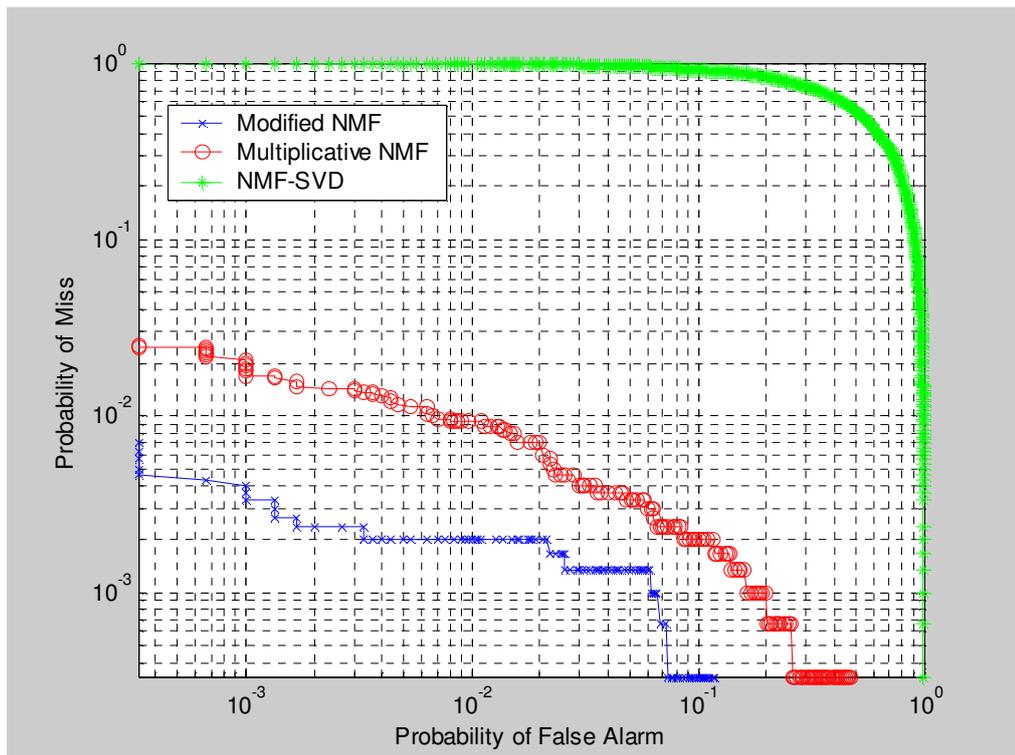


Figure 7.35. ROC curves for different methods when NMF dimension=35 and watermark power=20 db and image is subject to scaling attack of scaling factor=0.99

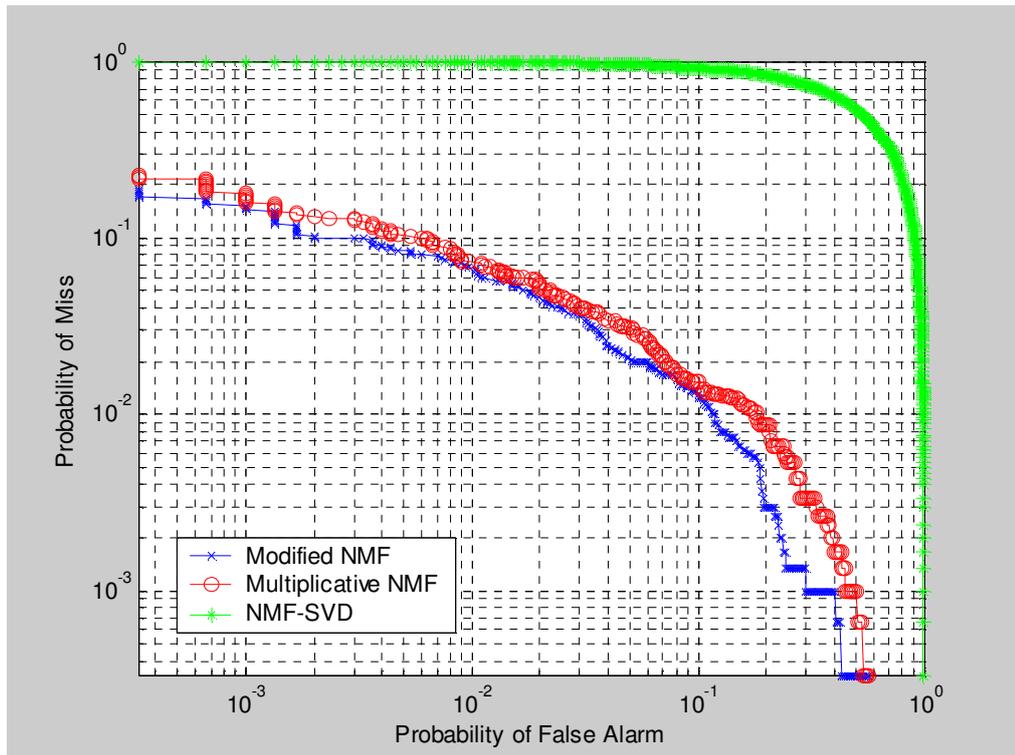


Figure 7.36. ROC curves for different methods when NMF dimension=35 and watermark power=25 db and image is subject to scaling attack of scaling factor=0.99

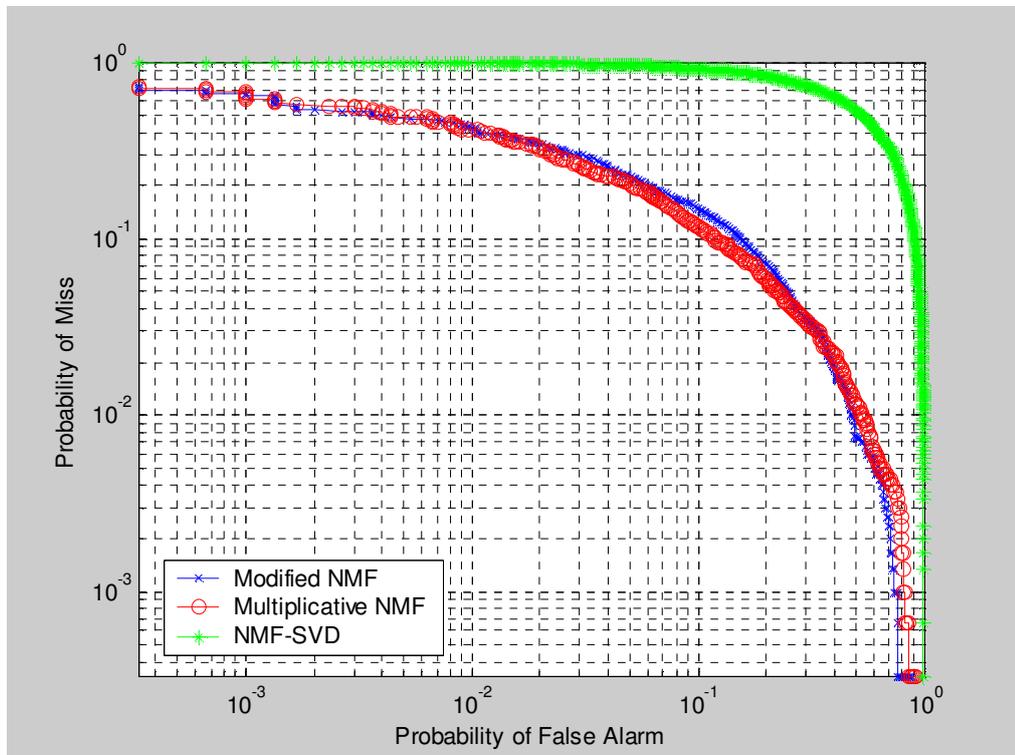


Figure 7.37. ROC curves for different methods when NMF dimension=35 and watermark power=30 db and image is subject to scaling attack of scaling factor=0.99

8. CONCLUSIONS

This study explores several NMF algorithms used for watermarking. The simulations were obtained both for multiplicative NMF algorithm, NMF-SVD algorithm and the newly proposed modified NMF algorithm. Results from these simulations for all algorithms are compared with each in terms of various aspects like NMF dimension, watermark power.

Simulations include several image attacks like additive white gaussian noise, JPEG compression, rotation and scaling. These attacks are simulated with different powers or parameters. These simulations are performed with an image database of 3000 gray scale images of size 512x512 pixels. In order to compare the three watermarking methods, same initial conditions, threshold values and watermarks are used.

It is derived from the simulations that the performances of NMF algorithms, both modified and multiplicative, depend on the NMF dimension. The relation between the NMF dimension and watermark verification performance is not linear, the best performance can be obtained for the NMF dimension range of 30-50. Apart from NMF dimension the watermark verification accuracy of the modified NMF depends on the watermark power. It is observed that the greater the watermark power, the higher accuracy in the watermark verification. It is found out from the simulations that modified NMF algorithm is more resilient to additive type of attacks, like AWGN attack, compared to geometric attacks like rotation or scaling. The modified NMF based watermarking verification is only acceptably accurate for very small distorting geometric attacks like 99 percent scaling.

When the simulation results for all three algorithms are compared modified NMF based watermarking is found out to have the highest accuracy in terms of watermark verification. After modified NMF, multiplicative NMF based watermarking has the highest and the NMF-SVD based watermarking has the lowest accuracy in terms of watermark verification. Only exceptional case is the JPEG compression attack. For the JPEG compression attacks modified NMF based watermarking has a lower performance when compared to other two watermarking methods. The higher performance of the modified

NMF based watermark verification is proposed to be related with the less uncertainty in the modified NMF since one of the resulting matrices is already fixed. Apart from the verification performance, since the iteration is done in one step for the modified NMF due to fix W matrix, the time required for modified NMF algorithm is almost half of the other two algorithms.

The main contribution provided by this thesis is the analysis of newly proposed NMF algorithm based on fixing the W matrix in the multiplicative NMF algorithm. With this motivation W matrix can be used as a secret key since the output of the NMF algorithm depends on the initial conditions. Another contribution provided by this thesis is the embedding of the watermark in the spatial domain in order to estimate the watermarked image in the NMF. Although the newly introduced modified NMF algorithm makes the watermarking algorithm simple and basic, it has a better performance than the multiplicative NMF.

To sum up, newly introduced NMF algorithm is a time efficient and simple algorithm for watermarking. Among various attacks, modified NMF based algorithm is less resilient to geometric attacks. This fact is proposed to be related with partially linear structure of the modified NMF since W matrix is fixed. When modified NMF is used instead of multiplicative NMF or two staged NMF-SVD, the accuracy of the watermark verification is higher. The future work will be to apply constraints on modified NMF or investigating an exact solution for the NMF – spatial domain transformation. So that there will not be need any estimation in the spatial domain for the NMF domain.

REFERENCES

1. Lee, D. D. and H. S. Seung, “Learning the Parts of Objects by Non-negative Matrix Factorization”, *Nature*, Vol. 401, No. 6755, pp. 778–791, October 1999.
2. Lee, D. D. and H. S. Seung, “Algorithms for Non-negative Matrix Factorization”, *Advances in Neural Information Processing Systems 13: Proceedings of the 2000 Conference*, Vancouver, 2001, Vol. 13, No. 6, pp. 556-562.
3. Tapper, U. and P. Paatero, “Positive Matrix Factorization: A Non-negative Factor Model with Optimal Utilization of Error Estimates of Data Values”, *Environmetrics*, Vol. 5, No. 2, pp. 111-126, 1994.
4. Albright, R., J. Cox, D. Duling, A.N. Langville and C. D. Meyer, “Algorithms, Initializations, and Convergence for the Nonnegative Matrix Factorization”, *NCSU Technical Report Math 81706*, 2007.
5. Mihcak, M. K. and V. Monga, “Robust Image Hashing via Non-negative Matrix Factorizations”, *Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings*, Vol. 2, pp. 225-228, 2006.
6. Browne, M., M. W. Berry, A. N. Langville, V. P. Pauca and R. J. Plemmons, “Algorithms and Applications for Approximate Non-negative Matrix Factorization”, *Computational Statistics & Data Analysis*, Vol. 52, No. 1, pp. 155-173, September 2007.
7. Hoyer, P. O, “Non-negative Matrix Factorization with Sparseness Constraints”, *Journal of Machine Learning Research*, Vol. 5, pp. 1457-1469, 2004.
8. Lin, C-J, “Projected Gradient Methods for Nonnegative Matrix Factorization”, *Neural Computation*, Vol. 19, No. 10, pp. 2756-2779, October 2007.

9. Cox, I. J., J. Kilian, T. Leighton and T. Shamoan, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions. on Image Processing*, Vol. 19, No. 10, pp. 2756-2779, October 2007.
10. Mihcak, M. K., R. Venkatesan and T. Liu, "Watermarking via Optimization Algorithms for Quantizing Randomized Semi-global Image Statistics", *ACM Multimedia Systems Journal*, 2005.
11. Hamza, A. B. and M. Ghaderpanah, "NMF-based Watermarking Scheme for Multimedia Protection", *IEEE International Symposium on Industrial Electronics*, Vol. 1, pp. 464-468, July 2006.
12. Chen, B. and G. W. Wornell, "Quantization Index Modulation Methods for Digital Watermarking and Information Embedding of Multimedia", *Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology*, vol. 27, no. 1-2, pp. 7-33, Feb. 2001.