INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

A Copyright Protection Technique Using Fractional Fourier Transform and Image Sharing

Arindam Dasgupta[1], Amit Kute[2]

[1]Professor, Dept. of IT, AVCOE Sangamner,
Maharashtra(India).
arindam.dasgupta.family@gmail.com

[2]Student of M.E. I.T., AVCOE Sangamner,
Maharashtra(India).
amitskute@gmail.com

Abstract: *Now a day's world is moving towards the digitization of all kind of data. There are many of possibilities of making attacks on those digitized data and hence it's become necessary to provide some security measure to such digitized data. Watermarking is one of the great schemes to provide security to digitized images and videos. To make these watermarking more robust and protective we introduce here in this paper a technique which involves Fractional Fourier Transform (FrFT) and part of Image sharing technique. In this paper we are using visual cryptography technique for image sharing. We are using this image sharing technique for generating two different shares namely master share and owners share. Owners share is registered at some certification authority which can be used for checking authenticity of image or digitized data in case of any attack. We use FrFT in our scheme to make this application robust so the watermark can retrieved without the help of any other image.*

Keywords: *Fractional Fourier Transform (FrFT), Image Sharing.*

1. INTRODUCTION

Digitization of information is become a vital aspect of information handling. Currently a day's tremendous amount of information can be created, holds on and transmitted thanks to rapid development in communication and transmission technology. To form this stuff possible some important issues are serving to improvement of functionality of digitization. These issues might include victorious operating and recognition of net, its low cost nature for transmission of information and therefore the distributed nature of storage devices. This stuff makes healthy surroundings for copying and modifying the digital contents. Thanks to this reason it raises a problem to supply security scheme to digitized information, so it'll be protected from modification. Currently this digitized information could also be audio, video or imaging.

Watermarking is one among the precise choices for digitized information security. As we have a tendency to are handling digitized information, digital watermarking plays important role in protection of digitized information and is that the wide used technique for information security. During this technique some other digital data is combined and more into digitized contents. This external data is nothing however the watermark just in case of videos and imaging. This digital watermark is acting as a digital signature and providing sense of possession and authentication of digitized image.

According to process of retrieval and extraction of digital watermark it is divided into three categories as:

1. Visible/ Non-blind Watermarking: In visible watermarking the watermark is semi-transparent data which overlays at some position original image. The practical working of visible watermarking is limited, because it requires some excess of storage for keeping

o

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

riginal image.

2. Semi-visible Watermarking: In this kind of watermark some extra information is used with watermark. So there is no need to exact watermark for checking authenticity of data.
3. Invisible/ Blind Watermarking: Invisible watermarking uses an invisible watermark which is embedded with original image and which can't be perceived with human eyes. That means it does not need the original image or adding information to retrieve the watermark.

To provide more robust system digital watermarking should satisfy some conditions and properties as:

1. The quality of image should not to be spoiled due to adding watermark and its quality is measured in Peak Signal to Noise Ratio (PNSR).
2. The watermark must be insightfully invisible.
3. The watermark must be protective in any way.
4. The watermark must be vigorous in case of common signal processing operation and geometric deformation.

There are various work domain in which watermark is get embed with digitized data. On the basis of these two domains, watermarking techniques are divided into 2 categories.

1. Spatial Domain Watermarking Techniques: In this technique pixel values of original image are directly get modified and then watermark is embed with these values.
2. Transform Domain Watermarking Technique: In this technique various transforms are use to perform transformation initially, such transforms include Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). Along with these transforms some extended type are also used such as Fractional Fourier Transform (FrFT) and Singular Value Decomposition (SVD). After performing transformations watermark is embedded by updating the values of coefficient.

The types of transform domain techniques are tougher in nature and hence protective to provide strong security against the various attacks, which make these techniques more robust than spatial domain techniques.

To safety of a secret image Moni Naor and Ali Shamir introduced a lossless technique for watermarking and this technique is known as Visual Cryptography (VC). In this paper we are going to deduce the technique using Fractional Fourier Transform, Visual Cryptography and Singular Value Decomposition [1].

Further paper is organized as follows: On section 2 there is a brief overview of previous work in this area. Section 3 gives the background of Fractional Fourier Transform, Visual Cryptography and Singular Value Decomposition. Section 4 gives the proposed scheme. Some modifications are given in discussions in section 5 and finally the conclusion of paper is stated in section 6.

2. EXISTING WORK

M.S. Wang and W.C. Chen introduced a hybrid DWT-SVD copyright protection scheme based on visual cryptography. The system introduced is working in following manner [6].

Original image is provided as input.

Step 1: Decompose original image into sub-bands by two level discrete wavelet transform.

Step 2: With the help of PRNG (Pseudo Random Number Generator) select list of pixel positions from LL2 sub-band randomly.

Step 3: from pixel positions 0 to n, perform SVD on a small window centered at each selected pixel.

Step 4: Use some singular values to generate feature vector.

Step 5: Apply K-means clustering algorithm to classify feature vector in R parts.

Step 6: Using clustering results generate master share.

Step 7: Use visual cryptography technique to generate ownership share. For use master share and secrete image.

At the time of extraction the hidden image can be retrieved by stacking of both shares at the time of any disagreement to ownership. This system is secure and robust against common signal processing attacks.

3. PROPOSED SYSTEM

3.1 Conceptual Background:

A. Fractional Fourier Transform:

Fractional Fourier Transform (FrFT) is the extension to the Fourier Transform which is from the class of time-frequency representation. The Fourier transform of continuous function F(t) of a continuous variable t, is denoted by $\hat{f}[F(t)]$ and is defined by,[8]

$$\hat{f}[F(t)] = \int_{-\infty}^{\infty} f(t)^{-2\pi Xt}\, dt \qquad \ldots\ldots (1)$$

Where X is also a continuous variable because t is integrated out

Volume 1, Issue II Mar. 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

$\hat{f}[F(t)]$ and id X.

Now the n^{th} order FrFT of signal is given by function,

$$F^n[f(x)] = \int_{-\infty}^{\infty} K_n(X,u)F(X)dx \qquad \ldots\ldots (2)$$

Where K_n(X, u) is kernel of transform and is defined according to three conditions respectively:

a. If α is not multiple of π
b. If α is multiple of 2π
c. If α+π is not multiple of 2π

Then the kernel is as follows:

$$K_\alpha(X,u) = \begin{cases} \sqrt{1-i\cot(\alpha)}\exp(i\pi(\cot(\alpha)(X^2+u^2) - 2\csc(\alpha)uX)) \\ \delta(u-X) \\ \delta(u+X) \end{cases}$$

…… (3)

Where n is the order of FrFT, α is rotation angle and relation between n and α is, $\alpha = n\pi/2$.

The proposed scheme is divided into two phases. At the first phase ownership share is registered and in second phase identification is performed.

B. Image Sharing:

We are using 2x2 schemes of VCS in this paper. Consider an image having size *MxN* and it is divided into two shares with size *2Mx2N*. Block of 2x2 pixels is to represent every pixel. At the time of encryption secret pixel is converted into two blocks belongs to respective share image to obtain share images. By stacking two corresponding blocks of pixel secret pixels are retrieved. Two share blocks of white secret pixel are similar in case of black secret pixel are complementary.

C. Singular Value Decomposition:

Here number of matrices is generated at each level of operation and to tackle with them we need same analysis tool. The requirement is fulfilled by singular Value decomposing (SVD). Which are tools used to analysis of matrices? Digital image is collection of matrices have non-negative scalar entries.

Now consider digital image A with order MxN where M<=N. SVD of digital image **A** is it's factorization along **X, S, Y** matrices such as,

$$\boldsymbol{A = X+S+Y^T} \qquad \ldots\ldots (4)$$

Here $\boldsymbol{X}$ and $\boldsymbol{Y}$ are orthogonal matrices and S is diagonal matrix with entries, $\boldsymbol{\lambda_1, \lambda_2, \lambda 3, \_\_\_, \lambda_{r+1}}$ satisfying condition that,

$$\boldsymbol{\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \_\_\_ \geq \lambda_r \geq \lambda_{r+1} = \_\_\_\_\_ = \lambda_m = 0} \qquad \ldots\ldots (5)$$

Where r is rank of $\boldsymbol{A}$.

Singular values are nothing but the eigenvalues of $\boldsymbol{AA^T}$ or $\boldsymbol{A^TA}$. These are the diagonal entries of S and are non-negative square root of eigenvalues.

1. Left singular vectors of A: these are eigenvalues of $\boldsymbol{AA^T}$ and are columns of $\boldsymbol{X}$.
2. Right singular vectors of A: these are eigenvalues of $\boldsymbol{A^TA}$ and are columns of $\boldsymbol{Y}$.

3.2 Shares Generation:

Consider, a host image H with size *M X N* and the secret image which is actually binary image of size *mXn* in this phase both shares are constructed.

A. Master Share Construction:

Step 1: Divide the host image H into 4X4 non-overlapping blocks

Step 2: Select mXn block with the help of Pseudo Random Number Generator seeded with key $\boldsymbol{K}$.

Step 3: Perform DFrFT with order $\boldsymbol{\alpha, \beta}$ on all mXn blocks.

Step 4: Collect singular values by performing SVD on each transformed block to generate $\boldsymbol{X}$.

Step 5: Develop binary map of $\boldsymbol{X}$ using,

$$B_{i,j} = \begin{cases} 0 & if\ ..X_{ij} < X_{av} \\ 1 & if\ ..X_{ij} \geq X_{av} \end{cases} \qquad \ldots\ldots (6)$$

Where $\boldsymbol{X_{av}}$ is average value of all pixels in $\boldsymbol{X}$.

Step 6: Now, master share is generated with size *2mX2n* is divided into non-overlapping 2X2 blocks. Now entries of these blocks are determined by following:

If $\boldsymbol{B_{ij}}$ is white pixel then, $m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

If $\boldsymbol{B_{ij}}$ is black pixel then, $m_i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

B. Ownership Share Construction:

'O' is ownership share and is generated using master share and binary secrete image $\boldsymbol{S}$. now consider O with size 2mX2n and divide it into 2X2 non-overlapping blocks. Consider the following rules to generate share 'O':

If $\boldsymbol{S_i}$ and $m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ then $O_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

If $\boldsymbol{S_i}$ and $m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ then $O_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

If $\boldsymbol{S_i}$ and

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

$m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ then $O_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

If S_i and $m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ then $O_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

The ownership share O should be registered with a certified authority (CA) for authentication.

3.2 Ownership Identification Phase

Ownership is detected in case of any attack on original host image as follows:

Step 1: Divide the host image ***H'*** into 4X4 non-overlapping blocks

Step 2: Select mXn block with the help of Pseudo Random Number Generator seeded with key ***K***.

Step 3: Perform DFrFT with order ***α, β*** on all mXn blocks.

Step 4: Collect singular values by performing SVD on each transformed block to generate ***X'***.

Step 5: Develop binary map of ***X'*** using,

$$B'_{i,j} = \begin{cases} 0 & if\ ..X'_{ij} < X'_{av} \\ 1 & if\ ..X'_{ij} \geq X'_{av} \end{cases} \quad \ldots\ldots (7)$$

Where X'_{av} is average value of all pixels in ***X'***.

Step 6: Now, master share is generated with size *2mX2n* is divided into non-overlapping 2X2 blocks. Now entries of these blocks are determined by following:

If B'_{ij} is white pixel then, $m_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

If B'_{ij} is black pixel then, $m_i = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Step 7: Retrieve the secret image S' by stacking the master share M' and the ownership share O kept by the CA.

Step 8: Divide the secret image S' into non-overlapping 2X2 blocks. Let us denote these blocks by s'.

Step 9: Get reduced secrete image S" as

$$S''_{ij} = \begin{cases} 0 & if\ -\sum_i \sum_j S'_{ij} < 2 \\ 1 & if\ -\sum_i \sum_j S'_{ij} \geq 2 \end{cases} \quad \ldots\ldots (8)$$

4. CONCLUSION AND FUTURE WORK

This system is more secure than previous techniques but still it has some more changes. Original image is of size *MXN* and the share is of size *nXn*. The size of the share changes at each level, thus easily identified as shares which requires some more information. The second one is, two share blocks of a white secrete pixel are similar while share blocks of black secret pixel are complementary. If pixels are black then it's ok but in case of white pixel there an overhead of maintain redundant data of white pixels. Original image is divided into number of shares. The outer pixels are having less possible combinations of black and white pixels. Hence this system manipulates pixels partially. Due to this the system may not gives exact output.

Our proposal, since pixels at the outer side of image are partially manipulated we can leave those pixels and consider the inner pixels only to generate shares. As we choose inner pixels excepting which are on at boundary the probability of combination is improved and hence there are less chances of partial manipulation.

References

[1] S. Rawat, B. Raman, "A Blind Watermarking Algorithm Based On Fractional Fourier Transform and Visual Cryptography", Signal Processing 92(2012), 1480-1491.

[2] C.C. Chang, J.C. Chung, "An image intellectual property protection scheme for gray level images using visual secret sharing strategy", Pattern Recognition Letters 23 (2002) 931–941.

[3] D.C. Lou, H.K. Tso, J.L. Lin, "A copyright protection scheme for digital images using visual cryptography technique", Computer Standards & Interfaces 29 (2007) 125–131.

[4] C.S. Hsu, Y.C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering 44 (2005) 077003

[5] T.H. Chen, C.C. Chang, C.S. Wu, D.C. Lou, "On the security of a copyright protection scheme based on visual cryptography", Computer Standards & Interfaces 31 (2009) 1–5

[6] M.S. Wang, W.C. Chen, "A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography", Computer Standards & Interfaces 31 (2009) 757–762

[7] M. Naor, A. Shamir," Visual cryptography", in: Proceedings of the Advances in Cryptology—EUROCRYPT'94, Lecture Notes in Computer Science, vol.950, Springer-Verlag, 1995, pp.1–12

[8] H.M. Ozaktas, O. Arikan, "Digital computation of the fractional Fourier transform", IEEE Transactions on Signal Processing 9 (1996) 2141–2149.

[9] B. Zhou, J. Chen, "A geometric distortion resilient image water-marking algorithm based on SVD", Chinese Journal of Image and Graphics 9 (2004) 506–512