A Cryptographic – Watermarking Technique for Securing 2D Logos using Diffuse Representation

Arthy R, Sivasankari M, Jegajothi B
Kamaraj College of Engineering and Technology

Abstract **- In the era of Internet, the multimedia data are more popularly accessed by anyone and there are chances for an unauthorized user to access the data. The combined process of cryptography and watermarking is proposed in this algorithm to provide both security and identity preservation. The cryptographic techniques are used to encrypt the data that converts the data into unreadable form. The watermarking is a technique that embeds the secret data into cover image. The proposed algorithm encrypts the binary secret information using diffuse representation algorithm. The encrypted image is then embedded into the cover image using DWT and SVD which embeds the information in the transform domain. The proposed algorithm is tested with various binary logos and the result shows that the PSNR and BER values are good. The algorithm ensures high percebility and improves the security level.**

Index Terms— Encryption, Decryption, Symmetric Encryption Algorithm, Diffuse Representation, Private Key Encryption Algorithm, Watermarking, Transform Domain, DWT, SVD, PSNR, BER

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

Visual Cryptography [12] is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can access it. Encryption does not of itself

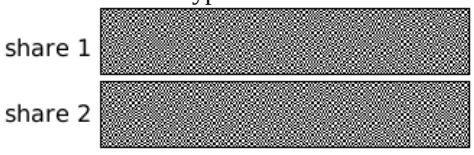

Fig. 1 – Shares

prevent interference,but denies the message content to the interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted.

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

Diffusion is an important parameter that must be measured to judge the encryption algorithm randomization. To test the security of the image encryption algorithm, two common measures may be used: Number of Pixels Change Rate (*NPCR*) and Unified Average Changing Intensity (*UACI*)

The [15], [16], [20] describes various visual cryptographic schemes for binary image, gray-colored images. The Extended Hamming Code is proposed in [14]. To represent the problem of pixel oversaturation a lossless and reversible encryption algorithm was proposed in [11]. The algorithm [17] presents the probabilistics model which adopts the (t, n) visual cryptography scheme. This model efficiently manages the dynamically changing user group.

The security level is upgraded using the bit level permutation technique in [18] for chas based image ciphers. This technique proves better performance because the bits are shuffled between different bit planes.

The error diffusion method [19] is used to provide the solution for management problem. Diffusion method adds a cover image to each share to make the share visible. The fallacy diffusion method is also used for shadow images [11]. This improves the quality of shadow image when compared to the existing algorithms.

The proposed algorithm in this paper is a symmetric encryption algorithm for binary images. The key used in symmetric encryption algorithm should not be disclosed publicly.

Watermarking is process of embedding secret information into the cover image. The watermarking can be done in spatial or transform domain. Spatial domain embeds the message in the pixels where as transform domain embeds a message by modifying the transform coefficients of the cover message as opposed to the pixel values. Ideally, transform domain has the effect in the spatial domain of apportioning the hidden information through different order bits in a manner that is robust. There are a number of transforms that can be applied to digital images, but there are notably three most commonly used in image watermarking. They are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

A Blind image watermarking technique propsed in [1] embed more number of watermark bits in the gray scale cover image without affecting the imperceptibility and increase the security of watermarks. A hybrid cryptographic and digital watermarking technique for securing digital im-

ages based on a Generated Symmetric Key was proposed in [2]. The method proposed in [3] for Plain image is very difficult to detect and cannot be visually distinguished.Digital Watermarking [4] is basically a phenomenon by which we can easily encrypt and decrypt a data in digital format so that it can be used by authorized users.In [5], data hiding and cryptographic techniques are combined into one secure simple algorithm. So, the original image is not mandatory at the time of watermark recovery. The algorithm specified in [6] focused on increasing the embedding capacity and improving security of the watermarks. But Encryption and Decryption process is complex. In [7], image classification was done which is on the basis of artificial intelligent scheme named as IWD (Intelligent Water drop System). Image used for classification is high resolution image. A watermarking scheme which that offers better security than Hwang's method is proposed in [8], so that, attackers will not be able to detect ownership information. The basic technique for watermarking colored images has been proposed [9] which takes the transformed domain for embedding. The algorithm proposed in [10] is based on the generation of a key as an image. It improves the confidentiality.

The rest of the paper is organized in the following manner. Section II discusses the proposed algorithm from which this paper has been developed. Section III discusses the encryption algorithm. Section IV discusses the embedding process. Section V discusses about the experimental results and Section VI gives the conclusion of the paper.

II. Proposed System

The visual cryptography technique is to encrypt the image and converts it into an invisible form. The proposed algorithm adopts this consept to increase the security of the secret image after embedding. The hacker even if extracts the embedded information will be unable to view the data since it is encrypted. This increases the security level.

The Fig. 2 describes the overall architecture of the proposed work. The encryption method used in this proposed work uses the diffuse representation method that was proposed by Houas et. al. The algorithm uses the single key. The number of sub images are denoted by numer of shares.

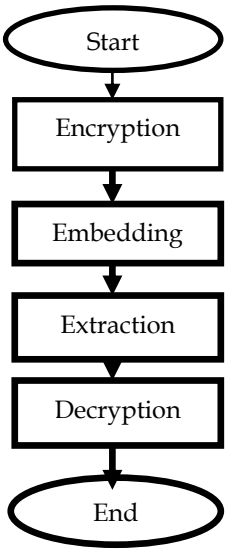

Fig. 2 – Overall Architecture

The encrypted image is then embedded into the cover iumage using DWT and SVD. The embedding process is described in section IV.

III. ENCRYPTION PROCESS

The diffuse representation proposed in [11] takes a binary image and divides it into number of non – overlapping subimages. The subimages are then mapped on to the original size. The mapping of the size of subimages to the original size is done in order to increase the security level. The subimage denotes the shares to be encrypted.

The encryption keys are generated from the subimages. The shares are then encrypted using the generated key.

Let I be the image and I_1 and I_2 are the subimages then the key for encryption β is given in equation (1).

$$\beta(i,j) = \frac{1}{2}\left[\left(a_1(i,j) + \frac{||I_1||_1}{\sqrt{64}}\right) + \left(a_2(i,j) + \frac{||I_2||_1}{\sqrt{64}}\right)\right] \quad (1)$$

The shares are then encrypted using the equation (2) and (3).

$$b = \beta(i,j) - a_1(i,j) \quad (2)$$

$$b = \beta(i,j) - a_1(i,j) \quad (3)$$

The encrypted shares are invisible and the shares are embedded into cover image.

IV. Embedding Process

The watermarking process in the proposed method embeds the encrypted secret logo into the cover image. The cover image is preprocessed to divide it into R, G, B channels. The green channel is choosen to embed the encrypted secret logo. The channel is choosen as green because the modification that is done in green channel will not be visible to the end user.

The embedding process can be done on spatial domain or in transform domain. The proposed algorithm embeds the encrypted secret logo in the transform domain. The embedding is done using DWT and SVD.

The Fig. 3 shows the embedding algorithm for the proposed work.

Algorithm 1:

/* Notations: m x m is the unitary matrix U, n x n unitary matrix V, m x n diagonal matrix S, watermarked image W_i, robustness factor α, secret image sec_i, combined matrix c, $N=2^k$
*/
Read 2D color image
Partition R,G,B planes
Choose G plane
Begin
If length N ie. f=(f1,f2,f3….fn)
Repeat upto 2-level DWT
for n=1 to N/2

$$a_n = (f_{2n-1} + f_{2n})/\sqrt{2}$$
$$d_n = (f_{2n-1} - f_{2n})/\sqrt{2}$$

end for
Divide the sub block matrix and secret image into U,S,V component

End
Repeat
$W_i = S + \alpha * sec_i$
Until i<S
c=W*U*V'
Apply inverse 2-level DWT
Combine R,G',B
End

Fig. 3 - Embedding Algorithm

The green channel is given as input for the embedding stage. The 2 level DWT is applied to find LL band of the channel. Initially 1-DWT is performed in the green channel to obtain CA(Average Co-efficient),CH(Horizontal Co-efficient),CV(Vertical Co-efficient),CD(Diagonal Co-efficient). The 1 level DWT is performed using 'haar' transform. Then 2-DWT is using 'haar' transform is performed in CA. As a result low (LL) band is obtained for the selected channel.

After the result of DWT, SVD algorithm is applied for the obtained LL and the secret image. This embedded matrices are split into three matrices, namely U,S,V. S matrix of the LL is used for embedding. Apply inverse 2-DWT and get the embedded green channel. Combine this green channel with red and blue channel.

The Fig. 4 shows the extraction process of the proposed algorithm.

Algorithm 2:

/* Notation:m*n is the unitary matrix U, n*n unitary matrix V, m*n diagonal matrix S, watermarked image S1, secret image , robustness factor α, secret image sec, combined matrix com, N = 2^k.
*/
Read the watermarked image
Partition R,G,B
Choose G channel
Begin
If length N ie. f=(f_1,f_2,f_3…..f_n)
Repeat upto 2-level DWT
For n=1 to N/2
$a_n = (f_{2n-1} + f_{2n})/\sqrt{2}$
$d_n = (f_{2n-1} - f_{2n})/\sqrt{2}$
end for
Decompose sub block matrix and secret image into U,S,V component
End
repeat
$sec_i = (S1 - s)/\alpha$
Until i<s
com=sec_i*U*V'
Apply inverse 2-level DWT
Combine R,G',B
End

Fig. 4 – Extraction Process

Extraction stage is the last stage of watermarking technique. Embedded image is given as input to the extraction stage. Initially 1-level DWT using 'haar' transform is performed in the sub block to obtained CA(Average Co-efficient), CH(Horizontal Co-efficient), CD(Diagonal Co-efficient). Then 2-DWT is using 'haar' transform is performed in CA. As a result low low(LL) of the selected sub block is obtained. After this, LL and the secret image obtained by SVD Algorithm that is to be embedded are split into three matrices, namely U,S,V.

The difference between of LL of the extraction stage and LL of the embedded stage is calculated. Apply inverse 2-DWT and get the original green signal. Combine the green channel with red and blue channel. Finally, the output is separated original image and secret image.

V. Experimental Results

The proposed algorithm is tested with benchmark images like lena, cameraman, Barbara and baboon The secret image taken for testing includes logos from various institutes.

The secret images are converted into binary image and then encryption is performed.

The encrypted binay images are embedded into the cover image using DWT and SVD.

The performance of the algorithm is calculated by using the metrics like Bit Error Rate (BER) and Peek Signal to Noise Ration (PSNR).

The PSNR is Peak Signal to Noise Ratio is an error comparison metrics to ensure the extraction watermark is not altered. The PSNR value is calculated using the formula mentioned in equation (4) and (5).

$$\mathbf{PSNR} = \mathbf{10\log_{10}(L\hat{}2/MSE)}$$

$$MSE = \sum\sum \frac{(original - extracted)^2}{H * W}$$

(4) and (5)

Where,
L - Maximum fluctuation of input image
H - Height of the object
W - Width of the object

The Bit Error Ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. The equation (6) shows the calculation of BER value.

$$BER = \frac{Number\ of\ pixel\ wrongly\ constructed}{Total\ Number\ of\ Pixels} * 100$$

(6)

The Table 1 tabulates the BER values for various input binary images having Lena as a cover image.

The ideal value of BER is relevant to zero and the result of the proposed system reflects the closest value to zero. The reveals that the encrypted and decrypted image looks alike.

TABLE 1
BER OF DECRYPTED IMAGE

Image	BER
KCET	0.0046
Annauniversity	0.0259
Apple	0.0229
Twitter	0.0320
Facebook	0.0137
VCET	0.0061

The Table 2 tabulates the PSNR values of various cover image for a binary secret image as KCET logo. The PSNR values are above 30 for all images which is also the ideal value.

TABLE 2
PSNR VALUES OF COVER IMAGE

Cover Image	PSNR
Lena	37.32
Cameraman	36.87
Baboon	33.81
Barbarra	33.80
Matlab	41.37

The PSNR values are related with the robustness factor in SVD. The SVD algorithm for embedding and extraction contains a robustness factor α, when varying α value the PSNR get differs. The equation (7) shows the formula for extraction using SVD.

$$S' = \frac{(S_1 - S)}{\alpha} \tag{7}$$

Where, S is a diagonal matrix and α is a robustness factor.

The Table 3 shows the result of PSNR value for different α values.

The Fig. 5 shows pictorially that α value when increased the PSNR values get decreased.

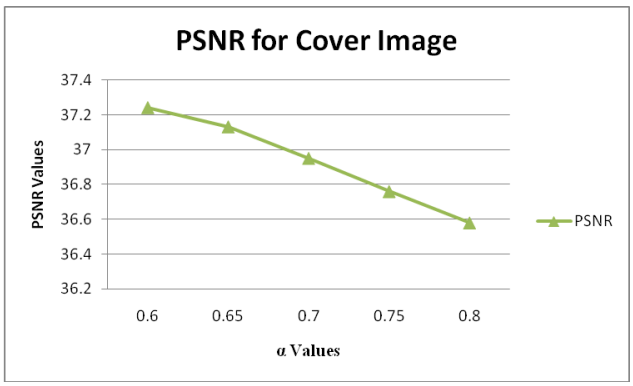

Fig. 5 – PSNR for Cover Image with repect to α value

The Fig. 6 states that when α values get increased BER values get decreased. This interpretation shows that α value is inversely propostional to BER & PSNR.

TABLE 3
BER AND PSNR VALUES

α	BER	PSNR
0.6	0.0214	37.24
0.65	0.0015	37.13
0.7	0	36.95
0.75	0	36.76
0.8	0	36.58

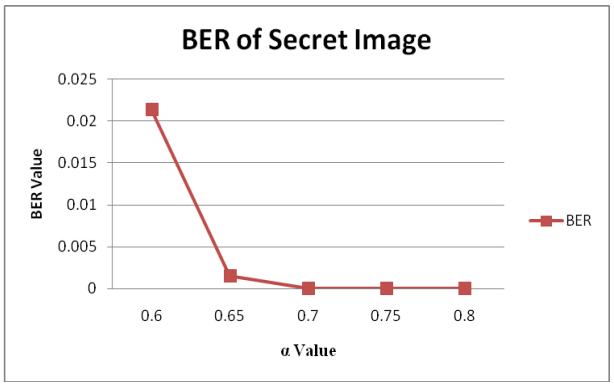

Fig. 6 – BER of Secret Image after decryption

VI. CONCLUSION

The increase in accessing of data in day to day life increases the need for secret in identity preservation. The security plays a vital role in Internet. Unauthorized should not have an access to the content. The proposed algorithm increases the security level since the keys are generated using the shares. The identity is also one another fact that has to be considered when a product is released to the customer. The watermarking technique when combained with the cryptography decreases the possibility of unauthorized users from accessing the data. The results shows the good BER value which ensures that the content is reterived back and the PSNR value proves that the impercebility of the cover image is maintained.

REFERENCES

[1] Preeti Gupta, " Cryptography based digital image watermarking algorithm to increase security of watermark data" International Journal of Scientific & Engineering Research, Volume 3, Issue 9,September 2015.

[2] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophi Gire, Jojo M.Eghan, and Narku Quaynor "A Hybrid Cryptograpic and Digital Watermarking Technique for securing Digital Images based on a Generated Symmetric Key". International Journal of Computer Applications (0975 –8887)Volume 94–No.19, May 2014.

[3] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophi Gire, Jojo M.Eghan, and Narku Quaynor "A Cryptograpic and Digital Watermarking Encryption Technique for securing and Authentication of Digital Images ". International Journal of Computer Applications (0975 –8887)Volume 119 –No.7, June 2015.

[4] Aseem saxena, Amit kumar sinha,Shashank chakrawarti,Surabi charu "Digital water marking using matlab". International Journal of Computer Applications (0975 –8887)Volume 119 –No.7, June 2014.

[5] Nirdesh Jain, Rashika Gupta " A Novel Approach for Digital Image Watermarking using cryptography". International Journal of Computer Applications (0975 –8877)Volume 119 –No.7, June 2014.
[6] Jasdeep Singh Bhalla, Preeti Nagrath " Nested Digital Image Watermarking Technique using blowfish encryption algorithm". International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2014-ISSN 2250-3153.
[7] Pooja Kulkarni, Shradda Bhise, Sadhana Khot " Review of Digital Watermarking Techniques". International Journal of Computer Applications (0975 –8887) Volume 109 –No. 16, January 2015
[8] Avi Chugh, Puneet Mittal " Security Enhancement by Integrating Image Classification with Digital Watermarking". Volume 4, Issue 4,April2014 ISSN: 2277 128XInternational Journal of Advanced Research in Computer Science and Software Engineering
[9] Naina Gaharwar, Reena Gunjan " Reversible watermarking for digital images using visual cryptography and pixel histogram shifting". International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information Technology ISSN 2320–088XIJCSMC, Vol. 4, Issue. 7,July2015, pg.185–193
[10] Achintya singhal, Kamred Udham Singh " Colored Image watermarking". International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 9, September 2015
[11] Xinpeng Zhang, Jing Long, Zichi Wang, Hang Cheng, "Lossless abd Reversible Data Hiing in Encrypted Images with Public-Key Cryptography", IEEE Transactions on Circuits and Systems for Video Technology, Volume 26, Issue 9, Sept 2016
[12] Neha K. Lakde and Dr. P. M. Jawandiya, "A Review of Various Visual Cryptography Schemes", International Journal of Research in Advent Technology, April 2016
[13] Amrane Houas, Zouhir Mokhtari, Kamal Eddine Melkani, Adelmalik Boussaad, "A Novel Binary Image Encryption Algorithm Based on Diffuse Representation", An International Journal on Engineering Science and Technology, Elsevier, Feb 2016
[14] Sudip Ghosh, Sayandip De, Santi Prasad Maity, Hafizur Rahaman, "A Novel Dual Purpose Spatial Domain Algorithm for Digital Image Watermarking and Cryptography using Extended Hamming Code", International Conference on Electrical Information and Communication Technology, IEEE, Jan 2016
[15] Niraj Kumar, Sanjay Agarwal, "An Efficient and Effective Lossless SymmetricKey Cryptography Algorithm for an Image", International Conference on Advances in Engineering and Technology Research, IEEE, Jan 2015
[16] Mona F.M. Mursi, May Salama, Manal Mansour, "Visual Cryptography Schemes: A Comprehensive Survey", International Journal of Emerging Research in Management & Technology, Nov 2014
[17] M. Sukumar Reddy, S. Murali Mohan, "Visual Cryptography Scheme for Secret Image Retrieval", Internation Journal of Computer Science and Network Security", Volume 14, No. 6, June 2014
[18] Chong Fu, Jun-Bin Huang, Ning-Ning Wang, Qi-Bin Hou, Wei-min Lei, "A Symmetric Choas-Based Image Cipher with an Improved Bit-Level Permutation Strategy", Entropy, February 2014
[19] Shekha Chenthara, Deepika M.P., Dr. Varghese Paul, "A Novel Approach on Color Extended VisualCryptography for General Access Structures using Error Diffusion", International Journal of Advanced Research in Computer and Communication Engineering", Volume 3, Issue 2, February 2014
[20] Suhas B. Bhagate, P.J. Kulkarni, "An Overview of Various Visual Cryptogrpahy Schemes", International Journal of Advanced Research in Computer and Communication Engineering", Volume 2, Issue 9, September 2013
[21] Xuehu Yan, Shen Wang, LiLi, Ahmed A. Abd EL-Latif, Zhiqiang Wei, Xiamu Niu, "A New Assessment Measure of Shadow Image Quality Based on Error Diffuse Techniques", International Journal of Information Hiding and Multimedia Signal Processing, Volume 4, Number 2, April 2013