A Noval Security Mechanism for Image Authentication and Copyright Protection

Thamodaran.K [1] Dr Kuppusamy.K [2]
1.Research Scholar, 2.Associate Professor,
Dept. of Computer Science and Engineering
Alagappa University, Karaikudi-630 003, India.

ABSTRACT

Encryption and watermarking are two primary and complementary technologies for protecting multimedia content. In this paper, we present a hybrid image protection scheme to establish a robust content-based authentication by using novel cryptosystem based on matrix transformation for generation of encryption key and copyright protection by using SVD based watermarking system. This paper suggests efficient method for encryption of image by self-invertible matrix with Hill Cipher algorithm. The Hill cipher algorithm is a symmetric cryptosystem for data encryption but cannot encrypt images. The novel cryptosystem uses randomly generated self-invertible matrix as an encryption key for each block encryption of an image and finding inverse of the matrix while decryption. This method having less computational complexity, because the inverse of the matrix is not required for decryption. For watermarking, we use SVD concept to provide a removable watermarking scheme for content based watermarking. The proposed scheme modifies the embedding strategy of SVD scheme. The proposed scheme yields higher security with superior encryption and robust to common image processing distortions. Experimental results show the effectiveness of the proposed hybrid scheme.

Keywords- Cryptosystem, Hill cipher, Image encryption, Self-invertible matrix, Watermarking, Singular value decomposition.

1. INTRODUCTION

The tremendous growth in digital image processing and network communications during the past decade have created a great demand for real-time secure image transmission over the Internet and through wireless networks. Image authentication differs from the traditional data authentication To exchange images between two parties on the network, it is very important to provide authentication and copyright protection. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Traditional text encryption schemes are unaffordable to encrypt images due to the bulky size of images. Also the decrypted image need not exactly be the same as the original image. Due to the characteristic of human perception, a decrypted image containing small distortion is acceptable as long as it does not affect the content of the image. The copyright protection issue can be resolved by embedding a piece of ownership information such as a logo or identity. The integrity of images can be ensured through content hash or content-based watermarks. Robustness of a watermark is the ability to extract the watermark correctly even if intentional or unintentional attacks are made on the watermarked image. To ensure security, only the authorized user should be allowed to embed and extract the watermark.

In the age of information technology, the problem of ensuring security to multimedia contents has been addressed by two different means, namely, media encryption and digital watermarking. The media encryption scrambles multimedia contents in order to make them unintelligible to any unauthorised user and ensures confidentiality. The digital watermarking embeds imperceptible information such as copyright in to media data, providing authentication of the content [1].Asymmetric encryption techniques are more slower than Symmetric techniques, because they require more computational processing power. The symmetric cryptography is normally used to encrypt private data for its high performance. Moreover, none of the most used symmetrical ciphering systems like DES, IDEA and AES make use of the most recent developments in information processing technology. There have been various data encryption techniques on multimedia data proposed in the literature[2],[3],[6].

Several digital watermarking algorithms have been reported in the literature . Based on the domain in which the watermark is embedded, image watermarking techniques can be divided into two categories namely spatial domain techniques and frequency domain techniques. The watermark can be secret information or a content hash or another image such as a logo. The watermark is added either in the spatial domain or frequency domain such as DCT domain or Wavelet domain or Fourier domain .In Christen Rey and Jean- Luc Dugelay have presented a survey of various watermarking algorithms that are used for content authentication of digital images. Though spatial domain watermarking schemes are simple they are less resilient to common image processing operations and offer lesser embedding capacity compared to frequency domain techniques. So frequency domain techniques are more popular than the spatial domain based methods [4].

A few years ago, a transform called the Singular Value Decomposition (SVD) was explored for watermarking . The SVD for square matrices was discovered independently by Beltrami in 1873 and Jordan in 1874, and extended to rectangular matrices by Eckart and Young in the 1930s. It was not used as a computational tool until the 1960s because of the need for sophisticated numerical techniques. In later years, Gene Golub demonstrated its usefulness and feasibility as a tool in a variety of applications. SVD is one of the most useful tools of linear algebra with several applications in image compression, and other signal processing fields[5],[7].

This paper explores the efficiency of image encryption using self-invertible matrix with Hill Cipher algorithm and SVD based watermarking and its security analysis. The rest of the paper is organized as follows: In Section 2, we give a brief description for Hybrid Scheme. In Section 3, Hill cipher , Modular Arithmetic and self-invertible matrix and algorithm are explained. Cryptosystem using hill cipher is given in section 4. SVD based watermarking algorithm is presented in Section 5. In Section 6, discusses the analysis using self-invertible matrix with Hill Cipher algorithm and SVD based watermarking that includes, measurement of encryption quality, key space analysis, statistical analysis, watermarked image quality, experimental results are also included and the last section concludes this paper.

2. HYBRID SCHEME

The proposed scheme suggests efficient hybrid image protection scheme to establish a robust content-based authentication by using novel cryptosystem based on matrix transformation for generation of encryption key and copyright protection by using SVD based watermarking system. Encryption of image is performed by self-invertible matrix with Hill Cipher algorithm. These method encompass less computational complexity as inverse of the matrix is not required while decrypting in Hill Cipher. For watermarking, we used SVD concept to provide a removable watermarking scheme for images.

3. HILL CIPHER, MODULAR ARITHMETIC AND SELF-INVERTIBLE MATRIX

In classical cryptography, the Hill cipher is a type of monoalphabetic(fixed substitutions) polygraphic substitution cipher. polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical to operate on more than three symbols at once. Each letter is first encoded as a number. Often the simplest scheme is used: A = 0, B =1, ..., Z=25, but this is not an essential feature of the cipher.

Consider a block of *m* letters is as a vector of n dimensions, and multiplied by a *(m × m)* matrix, modulo 26. Let *m* be a positive integer, consider *m* linear combinations of the *m* alphabetic characters in one plaintext element and produce *m* alphabetic characters in one ciphertext element. Then, an *(m × m)* matrix *A* is used as a key of the system such that *A* is invertible modulo 26. Let *aij* be the entry of *A* . For the plaintext block $x=(x_1, x_2,\ldots, x_m)$,where=$(x_1, x_2,\ldots, x_m)$ are the numerical equivalents of *m* letters and a key matrix *A* , the corresponding ciphertext block $y=(y_1, y_2,\ldots, y_m)$ can be obtained as follows.

Encryption :

$$(y_1, y_2,\ldots, y_m) =(x_1, x_2,\ldots, x_m)\, A(\text{mod } 26) \quad \ldots(1)$$

Where

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix}$$

The ciphertext is obtained from the plaintext by using a linear transformation.|

Decryption:

The reverse process of enciphering,the deciphering is obtained , by

$$(x_1, x_2,\ldots, x_m) =(y_1, y_2,\ldots, y_m)\, A^{-1}(\text{mod } 26) \quad \ldots(2)$$

where

$$A^{-1} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix}^{-1} (\text{mod } 26)$$

Here the block length is *m* ,there are 26^m different *m* letters blocks possible, each of them can be regarded as a letter in a 26^m letter alphabet. Hill's method amounts to a monoalphabetic substitution on this alphabet[8] .

The modular arithmetic operation presented here are addition, subtraction, unary operation, multiplication and division. Based on this the self invertible matrix for Hill cipher algorithm is generated. As Hill cipher decryption requires inverse of the matrix, we suggest the use of self-invertible matrix generation method while encryption with the Hill. The algorithm generates *n*× *n* matrix where *n* is even and utilized for generating a self-invertible matrix. Let *s* be the seed for generating the random number, *t* be the multiplier generating the random number,*p* the modules(prime no.)and *k* is the scalar constant.

4. CRYPTOSYSTEM USING HILLCIPHER ALGORITHM

Step1:

Generate (nXn) matrix, where n is a even value; which is used for generating Self Invertible matrix. Let *s*=seed value, *t*=multiplier for generating random number, *p*=mod values(prime no.)and *k*=scalar constant.

Step2:

Create a random matrix of (n/2 X n/2),

namely $A_{11.}$

.

Stept3: Create A_{22}= -A_{11}

Step4: Create A_{12} as A_{12}= k(I-A_{11}).

Step5: Create A_{21} as $A_{21=}$ 1/k(I+A_{11}),finally, A is obtained.

In the method of generation of self-invertible matrix, the matrix used for the encryption is itself self-invertible. So, in the proposed cryptosystem , we need not to find inverse of the matrix while decryption. Mostly in this cryptosystem, the different key matrix is generated for each block encryption instead of keeping the key matrix constant,which increases the secrecy of data. For generating different key matrix each time, the encryption algorithm randomly generates the seed number and from this key matrix is generated.The whole matrix is considered as the cipher key, and should be random provided that the matrix is invertible. The Hill cipher algorithm cannot encrypt images that contain large areas of a single color. Thus, it does not hide all features of the image The novel cryptosystem uses randomly generated self-invertible matrix as an encryption key for each block encryption and also this method eliminates the computational complexity involved in finding inverse of the matrix while decryption. Hill cipher can be adopted to encrypt grayscale and color images. For grayscale images, the modulus will be 256. In the case of color images, first decompose the color image into (R-G-B) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted color image.

5. SVD-BASED WATERMARKING SCHEME

In our scheme,SVD-based watermarking scheme is used to embed watermarks in to images, and its hidden watermarks can resist various attacks. The proposed scheme is using content watermark based on the SVD of image , for an image (N× N) pixels and a watermark (P×P) pixels. In our scheme, the image is first divided into(N×N) non-overlapping blocks. The robustness of the hidden watermark and the scheme maintains the image quality of the watermarked image. To make sure the order of non-zero coefficients in S will not be changed and the hidden watermark can be successfully extracted. The proposed embedding algorithm is presented below:

5.1. Embedding Algorithm

Step1: The matrix is first divided into (N× N) non-overlapping blocks.

Step 2: Perform SVD operation on matrix (N× N) ,to generate its corresponding Uj , Sj, and Vj matrices.

$$\text{Let Sj} = \begin{bmatrix} S_1 & 0 & 0 & 0 \\ 0 & S_2 & 0 & 0 \\ 0 & 0 & S_3 & 0 \\ 0 & 0 & 0 & S_4 \end{bmatrix}_J$$

Step 3: Embed the Watermark in the given image.

Step 4: Perform SVD inverse operation on Uj , S’j, and Vj matrices to reconstruct the watermarked image , which is equal to Uj × S’j × V^Tj .

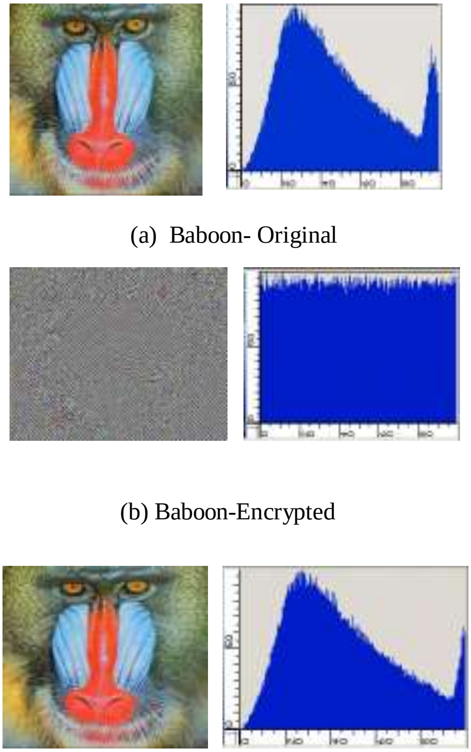
5.2. Extracting Algorithm

The watermark extraction Algorithm is the reverse of embedding Algorithm .

6. EXPERIMENTAL RESULTS

In this system ,Visual Studio .NET (C#.Net) and Photoshop7 are used for implementation and testing the image processing experiments.

Fig(1):Baboon original and processed images and its corresponding Histograms are paired from (a) to (g)



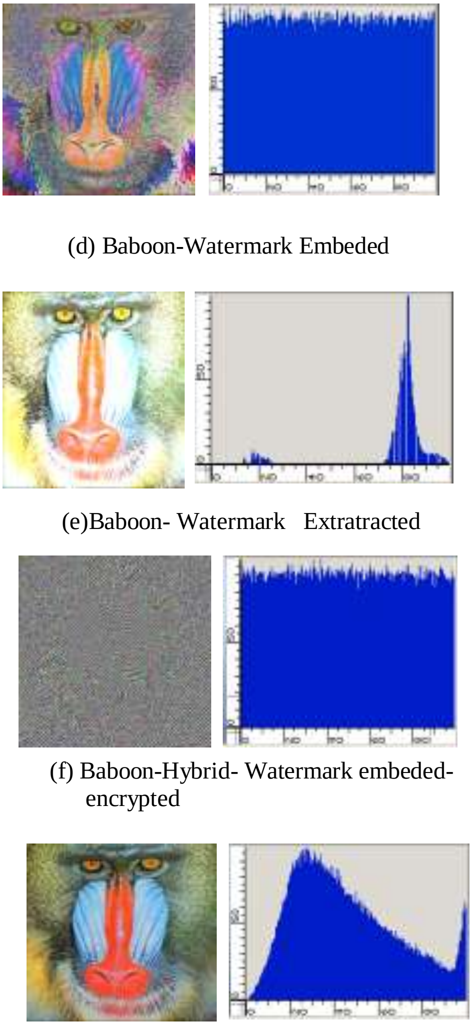
(a) Baboon- Original

(b) Baboon-Encrypted

(c)Baboon-Decrypted

Table -1: Correlation Coefficient for the two adjacent pixels in Original, Watermarked, Encrypted , Hybrid Watermarked and Encrypted Images.

Image	Original	Water marked Image	Encrypted Image	Hybrid Water marked and Encrypted Image
Baboon	0.9281	0.0393	0.0192	0.0052
Lena	0.9625	0.0247	0.0285	0.0084
House	0.9318	0.0208	0.0179	0.0059
Girl	0.9736	0.0521	0.0263	0.0042
Pepper	0.9465	0.0313	0.0361	0.0073



(d) Baboon-Watermark Embeded

(e)Baboon- Watermark Extratracted

(f) Baboon-Hybrid- Watermark embeded-encrypted

(g)Baboon-Hybrid- Watermark extracted –decrypted

Table -2: PSNR of watermarked , Encrypted, Hybrid Watermarked and Encrypted Images(in dB)

Image	Water marked Image	Encrypted Image	Hybrid Watermarked and Encrypted Image
Baboon	31.28	11.68	11.37
Lena	33.62	12.27	12.11
House	34.74	11.79	10.23
Girl	30.57	10.86	10.29
Pepper	33.94	12.38	12.20

7. CONCLUSION

The Hill cipher with self invertible matrix method generations self-invertible matrix, while encryption. So, we need not to find inverse of the matrix while decryption and time also reduced.When we change the seed and key value the system does not decrypt the image properly which gives more security.The SVD based watermarking gives more robust and quality images.When we consider the hybrid Hill cipher with self invertible matrix method SVD based watermarking system gives better results based on PSNR and Correlatin coefficients than normal methods.

REFERENCES

[1].G. Boato, N. Conci, V. Conotter, F.G.B. De Natale and C. Fontanari,”.Multimedia asymmetric watermarking and encryption” ELECTRONICS LETTERS .24th April 2008 Vol. 44 No. 9.

[2] Diaa Salama Abdul. Elminaam1, Hatem Mohamed Abdul Kader2 and Mohie Mohamed Hadhoud3 , “Performance Evaluation of Symmetric Encryption Algorithms”,. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008Pp 280-286.

[3]. Behrouz A.Forouzan , “Cryptography and Network Security ”TMH, 2010.

[4]. Christen Rey and Jean-Luc Dugelay, “A Survey of Watermarking Algorithms for Image Authentication,” EURASIP Journal on Applied Signal Processing, Vol. 6, pp. 613-621, 2002.

[5]. Alexander Sverdlov ,Scott Dexter and Ahmet M. Eskicioglu ,” Robust DCT-SVD Domain Image Watermarking for copyright protection: Embedding data in all frequencies”,proceedings of the 13th Europian Signal Processing Conference ,Antalya, turkey,September,2005.

[6] I Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda,” Image Encryption by Novel Cryptosystem Using Matrix Transformation”,IEEE computer society ,2008, First International Conference on Emerging Trends in Engineering and Technology. Pp 77-81.

[7] Chin-Chen Chang, Chia-Chen Lin , Yih-Shin Hu “ An SVD oriented watermark embedding scheme with high qualities for the restored images”, International Journal of Innovative Computing, Information and Control ICIC International °c 2007 ISSN 1349-4198 Volume 3, Number 3, June 2007 pp. 609—620.

[8] Petersen, K., Notes on Number Theory and Cryptography. http://www.math.unc.edu/Faculty/petersen/Coding/cr2.pdf.