Volume 2, No. 1, Jan-Feb 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Polynomial Based Secret Sharing Scheme for Image Encryption Based on Mathematical Theorem

A. Kalai Selvi*
Associate Professor in computer science
S.T.Hindu College,
Nagercoil, India,
kalaisthc@gmail.com

Dr.M.Mohamed Sathik
Associate Professor in computer science
Sadakathullah Appa College,
Tirunelveli, India,
mmdsadiq@gmail.com

Abstract: With a ever increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one of the way to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine and military communications. This paper proposes image encryption using secret sharing scheme. According to this process there are two levels of encryption. The first level, generates the random polynomial of degree (t-1) , where t is a threshold value. The constant term is taken as the secret. In the second level construct the transformation matrix using secret and primitive root theorem. This matrix is used for encryption purpose. Experimental results and security analysis shows that the proposed algorithm offers good resistance against brute force attack and statistical crypt analysis.
Keywords- Zone , block , secret , transformation matrix , encryption.

I. INTRODUCTION

Information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access. With a ever increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one of the way to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine and military communi cations. 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 [1].

Many encryption schemes have been analyzed as possible solution systems. The basic ideas can be classified into three major types: position permutation [2]&[3], value transformation [4]&[5] and the combined form [6]. The Novel crypto system [7] uses randomly generated self invertible matrix as an encryption key for each block encryption. The resulting image from the algorithm is scrambled using a random matrix which is used as another secret key. This increases the secrecy of data. This method encompasses less computational complexity during decryption, as self invertible matrix [8] is used as key. With the rapid development of Internet technology, communication using multimedia implement secure communication, such as photographs from military satellite, drawings of military establishment. On the other hand, some data transmitted are characterized in terms of privacy, integrity and authenticity thought public network. Thus keeping secret of data is getting more and more attention in the present paper an innovative technique for image encryption is proposed based on the random generation of polynomial. The new algorithm provides image encryption at two levels and hence security against the image is achieved at low computational overhead.

II. SECRET SHARING

Any method of dividing a secret into multiple (that is "n") participants is secret sharing. Each person receives a piece of the secret and the secret can be recovered by combining some or all of the shares. The secret is in the form of polynomial of degree "t-1", where "t "is the number of keys needed to get the secret (i.e., threshold value). The polynomial is expressed mathematically as follows.

$$F(x) = \sum_{i=0}^{t-1} a_i x^i \quad (1)$$

Where a_i is a coefficient.

A. *Secret Process*

A (t,n) threshold secret sharing scheme [1,2] is a cryptographic primitive used to distribute a secret "s" to "n" participants in such a way that a set of "t" or more participants can recover the secret "s" and a set of (t-1) or fewer participants cannot recover the secret "s".

The secret to be shared consists in text data , but also images can be considered. The first scheme to share images was due to Naor and Shamir [3] and it is called visual cryptography. It is based on visual threshold schemes t of n.

In this method, the coefficients a_0, a_1, …,a_{t-1} are randomly generated .The polynomial with the coefficients a_0,a_1, ….,a_{t-1} of degree (t-1) is represented as follows.

$$F(x) = a_0 + a_1 x + \ldots.. + a_{t-1} x^{t-1}. \quad (2)$$

Let the registered participant be "n" and let $t < n$, where t is a threshold value. Each participant has their own identity value ID_i (i = 1 to n) . The function value of the polynomial for the input of participant's ID value is performed. Each function value is given to the

© 2010, IJARCS All Rights Reserved

corresponding participant. The function value for ID_1 is share1; the function value for ID_2 is share2 and so on. The sender sends share1 to the participant for ID_1, share2 for ID_2 and so on. The process is clear from the following flowchart.

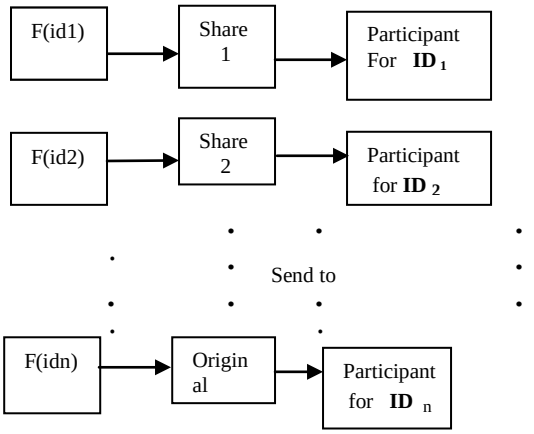

Figure.1. Secret process flow chart

B. Polynomial Generation

The first level of encryption is based on polynomial generation. The polynomial used in this level is generated at random and is of degree (t-1), where t is a threshold value. This could be expressed as follows.

$$F(x) = \sum_{i=0}^{t-1} a_i x^i \qquad (3)$$

Where a_i ia randomly generated coefficients.

III. ENCRYPTION TECHNIQUES

This technique is based on the following mathematical theorem.

A. Theorem

A primitive root of a number is the one whose powers generate all the integers from 0 to p-1. That is if " a" is a primitive root of the primitive number "p" then the number "a mod p" , "a^2 mod p" ….. "a^{p-1} mod p" are distinct and consists of integers from I through p-1 in some permutation.

B. Block Construction

Two block matrix of size 6 x 6 are constructed from the theorem, When p = 7 and a = 3

a1 = (3 2 6 4 5 1)

when p = 7 and a = 5

b1 = (5 4 6 2 3 1)

The first block matrix "A" , a1 values are taken as the first row elements. Then add the adjacent elements of the first row to get the second row. Then the same procedure is applied with the second row to get the third row. And finally this procedure is applied with the fifth row to get the sixth row. Next apply this procedure with b1 values to get the second block matrix "B".

C. Zone Construction

The zone matrix " M " of size 216 x 216 is computed by using the following formulas.

$$i = (i_1 - 1) * t^{r-1} + (i_2 - 1) * t^{r-2} + \ldots\ldots\ldots + (i_{r-1} - 1) * t^1 + i_r * t^0$$

$$j = (j_1 - 1) * t^{r-1} + (j_2 - 1) * t^{r-2} + \ldots\ldots + (j_{r-1} - 1) * t^1 + j_r * t^0$$

$$M(i, j) = (a_{1,i_1-1} \oplus a_{2,i_2-1} \ldots\ldots \oplus a_{r,i_r-1} \oplus a_{r+1,j_1-1} \oplus a_{r+2,j_2-1} \oplus \ldots\ldots \oplus a_{2r,j_r-1}) \bmod 256$$

For $i_k = 1,2,\ldots t$, $j_k = 1,2,\ldots t$, k = 1 , 2 … r.

Here t = 6, r = 3 , $a(i, j) \in A, B$

D. Transformation Matrix

The Transformation matrix has the following form.

$$T = \begin{pmatrix} M(X1) & M(X2) & M(X3) \\ M(Y1) & M(Y2) & M(Y3) \\ M(Z1) & M(Z2) & M(Z3) \end{pmatrix}$$

Where

X1 = (S * A) Mod 256
X2 = (S * B) Mod 256
X3 = ((S+1) * A) Mod 256
Y1 = ((S + 2) * A) Mod 256
Y2 = ((S + 2) * B) Mod 256
Y3 = ((S + 3) * A) Mod 256
Z1 = ((S + 4) * A) Mod 256
Z2 = ((S + 4) * B) Mod 256
Z3 = ((S + 5) * A) Mod 256
M(X) → Zone of X
S → Secret
A , B → Block matrix 6 x 6

E. Encryption Process

The Transformation matrix is XOR with the image matrix to get the encrypted image.

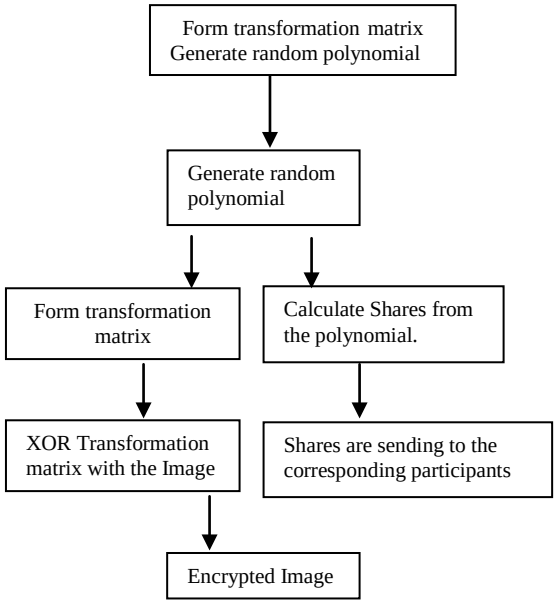

Figure.2. Encryption process flow chart

© 2010, IJARCS All Rights Reserved

IV. DECRYPTION PROCESS

A. Reconstruction

Each participant accepts the share from the sender for reconstructing the secret. The participant who is having the identification value ID_1 accepts the share y(1), the participant having the identification value ID_2 receives the share y(2) and so on. Only t shares are enough to reconstruct the secret. The combiner receives t shares y(1), y(2) , …y(t) and the polynomial is reconstructed by using Lagrange interpolation formula . The Lagrange interpolation formula is given below.

$$F(x) = \sum_{i=0}^{t-1} y(i) \prod_{\substack{0 \le k \le t-1 \\ k \ne i}} \frac{x - x_k}{x_i - x_k} \qquad (5)$$

Where x_1 , x_2 , … x_t are the identification values. F(x) → The reconstructed polynomial . t → Threshold value

B. Decryption Process

The receiver reconstructs the polynomial from the shares of the participants using Lagrange interpolation formula. The mean value is evaluated from the reconstructed polynomial. Next the cipher text is decrypted with the mean value to get the original text. The following flowchart explains this.

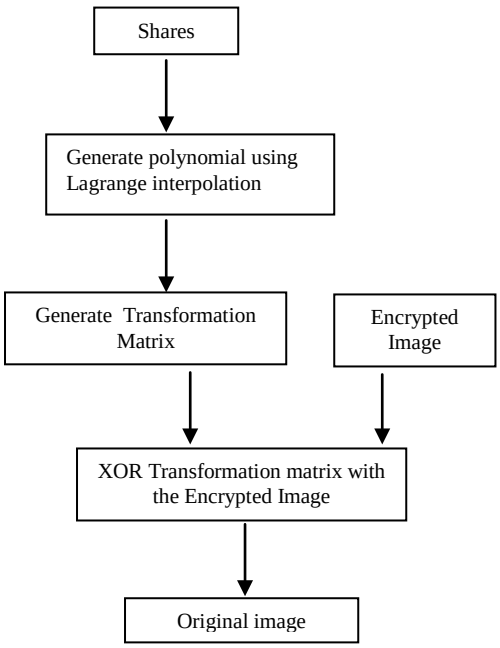

Figure.3. Decryption process

V. ENCRYPTION ALGORITHM

A. Take the Original Image.
B. Randomly generate the polynomial of degree (t-1)
C. Construct the Transformation Matrix
D. XOR Transformation matrix with Image matrix
E. The threshold value t , identification value of the participants ID (ID_1, ID_2, …, ID_n) and the Encrypted image are given in public.
F. Calculate the function values $F(ID_1)$,$F(ID_2)$, ..$F(ID_n)$.
G. Send $F(ID_i)$ to the participant having the ID value ID_i , where i = 1 to n.

VI. DECRYPTION ALGORITHM

A. Reconstruct the polynomial from "t" shares using Lagrange interpolation.
B. Construct the Transformation Matrix
C. XOR Transformation matrix with Encrypted Image matrix
D. Get the Original Image

VII. SAMPLE IMAGES

Figure 4: Leena Image

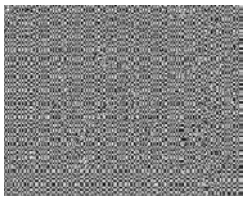

Figure 5 : Encrypted Leena

Figure 6: Cameraman

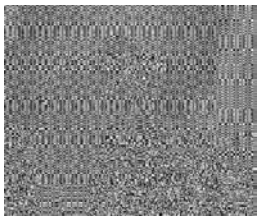

Figure 7: Encrypted Cameraman

Figure 8: Gold hill

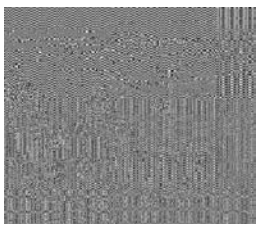

Figure 9: Encrypted Gold Hill

VIII. ANALYSIS

In this investigation, the set of criteria for analyzing the performance of encryption algorithms namely, information entropy analysis and Encryption Quality analysis.

A. Information Entropy

The entropy H of symbol S can be calculated using the following equation.

$$H(S) = -\sum_{i=0}^{N-1} p(s_i) \log_2 p(s_i),$$

Where $p(s_i)$ represents the probability of symbol s_i.

If the information entropy of encrypted image becomes larger, image distribution of gray scale will be more uniform. By calculation, the information entropy of Leena encrypted image is equal to 7.9972, which means that information leakage in the encrypted process is negligible and the encryption system is secure from the entropy attack.

B. *Encryption Quality Analysis*

One of the important factors in examining the encrypted image is the visual inspection where the highly disappeared features of the image the better the encryption algorithm.

© 2010, IJARCS All Rights Reserved

But depending on the visual inspection only is not enough in judging the complete hiding of the content of the data image. So, other measuring techniques are considered to evaluate the degree of encryption quantitatively.

With the implementation of an encryption algorithm to an image, a change takes place in pixel values as compared to the values before encryption. Such change may be irregular. Apparently this means that the higher the change in pixel values, the more effective will be the image encryption and hence the quality of encryption. So, the quality of encryption may be expressed in terms of the total deviation in pixel values between the original image and the encrypted one. The measuring factor considered here is maximum deviation.

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images. The steps of the measure will be done as follows:

[a] Count the number of pixels of each greyscale value in the range from 0 to 255 and present the results graphically for both original and encrypted images.

[b] Compute the absolute difference or deviation between the two curves and present it graphically.

[c] Count the area under the absolute difference curve, which is the sum of deviations (D) and this represents the encryption quality. D is given by the following equation:

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i$$

Where h_i is the amplitude of the absolute difference curve at value i. Of course, the higher the value of D, the more the encrypted image is deviated from the original image. The Maximum Deviation of this proposed algorithm is computed and is tabulated as follows.

Table2: Maximum deviation Table

Image	Size	Maximum Deviation
Leena	256 x 256	37965
Cameraman	256 x 256	64880
Gold Hill	512 x 512	182255

IX. CONCLUSION

In the new algorithm a polynomial is generated randomly. It is almost impossible to extract the original image in the proposed method even if the algorithm is known. In this algorithm, the image is encrypted after a number of rounds, which makes the computation more complex. Compared with the encryption schemes[10] based on the secret sharing , the size of the shares is far smaller with the size of the image.

X. REFERENCES

[1] Imai H.Hanaoka G., Shikata J., Otsuka A., Nascimento A.C., "Cryptography with information theoretic Security", Information Theory Workshop, 2002, Proceedings of the IEEE, 20 - 25 Oct 2002.

[2] DingWei, QiDongxu: Digital image transform, information hiding and camoufiage technique. Journal of computers. 1998 21:838–843, September, 1998.

[3] A. Shamir, How to share a secret. Communication of the ACM 22 (1979) : 612 - 613.

[4] M.Naor, Visual Cryptography. In Proceeding of - Eurocrypt '94, (1994) 441 – 449.

[5] Cao Zhenfu: A threshold key escrow based on public key cryptosystem. Science in China (Series E) , 200144: 441 – 448, April, 2001.

[6] Shannon, C.E.:Communication Theory of secrecy systems. Bell System Technical Journal.1994 28:656–715,April, 1994.

[7] Bidhudendra Acharya, Sarat Kumar Patra and Ganapati Panda " A Novel Cryptosystem Using Matrix Transformation", Proceedings of SPIT-IEEE Colloquium & International Conference Vol 4, pp. 92 – 95, 2008.

[8] Bidhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra and Saroj Kumar Panigrahy. "Novel Methods of Generating Self Invertible Matrix for Hill Cipher Algorithm", International Journal of Security (CSS Journals). Vol 1, Issue. (1), pp. 14 – 21, 2007.

[9] Ling Wang, Qun Ye, Yaoqiang Xiao, Yongxing Zou, Bo Zhang "An Image Encryption Scheme Based on Cross Chaotic Map" Proc. IEEE 2008 Congress on Image and Signal Processing, 2008, 22-26.

[10] Jeyamala C, Subramanyan B Raman G S, "A Real time Image Encryption Techniques Based on Discrete Logarithms" L.M. Patnaik and Venugopal K.R (Eds.), ICIP- 2010, Pages 107-112 (c) 1K International Publishing House Pvt.Ltd., New Delhi.

© 2010, IJARCS All Rights Reserved