Secret Sharing Scheme for Image Encryption Based on Primitive Root Theorem

A. Kalai Selvi[1] and M. Mohamed Sathik[2]

[1]*Associate Professor in Computer Science, S. T. Hindu College, Nagercoil, India*
[2]*Principal, Sadakathullah Appa College, Tirunelveli, India*

kalaisthc@gmail.com, mmdsadiq@gmail.com

Abstract

In recent years, there has been increasing trend for multimedia applications to use delegate service providers for content distributions. These delegate services have brought new challenges to the protection of multimedia content confidentiality. Encryption can be used to hide information from unauthorized individuals, either in transit or in storage. This technique transforms the content into unintelligible and unviewable format. 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: *Encryption, decryption, transformation matrix, secret*

1. Introduction

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. 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.

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.

2. 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.

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

Where a_i is a coefficient.

3. 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 $a_0, a_1, \ldots, a_{t-1}$ are randomly generated .The polynomial with the coefficients $a_0, a_1, \ldots, a_{t-1}$ of degree (t-1) is represented as follows.

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

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 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.

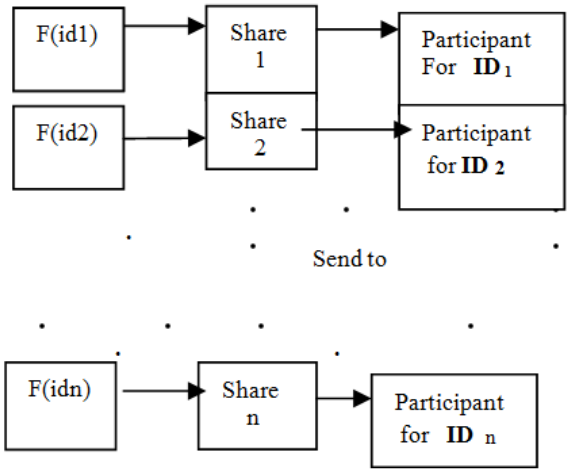

Figure 1. Secret Process Flow Chart

4. 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.

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

Where a_i ia randomly generated coefficients.

5. Encryption Techniques

This technique is based on the following mathematical theorem.

5.1 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.

5.2 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".

5.3. Zone Construction

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

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

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

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

For $i_k = 1,2 \ldots t$, $j_k = 1,2,\ldots t$, k = 1 , 2 … r.
Here t = 6, r = 3 , $a(i, j) \in A, B$

5.4 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

5.5 Encryption Process

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

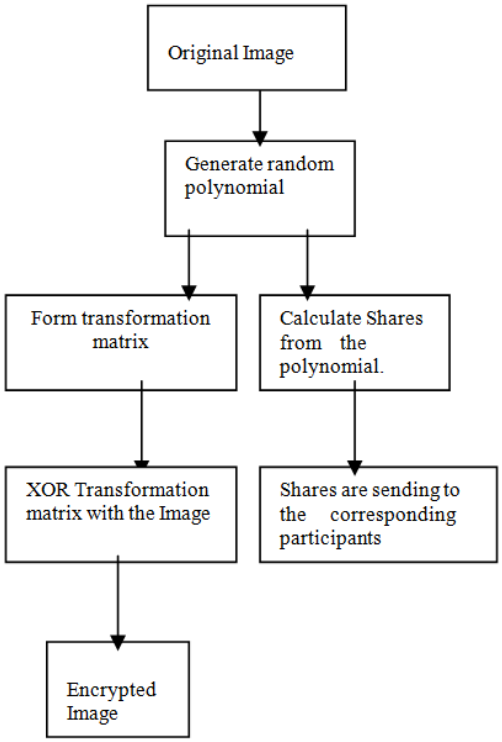

Figure 2. Encryption Process Flow Chart

6. Decryption Method

6.1 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

6.2 Decryption Process

The receiver reconstructs the polynomial from the shares of the participants using Lagrange interpolation formula. The transformation matrix is reconstructed from the polynomial. Next the encrypted image is decrypted with the transformation matrix to get the original image. The following flowchart explains this.

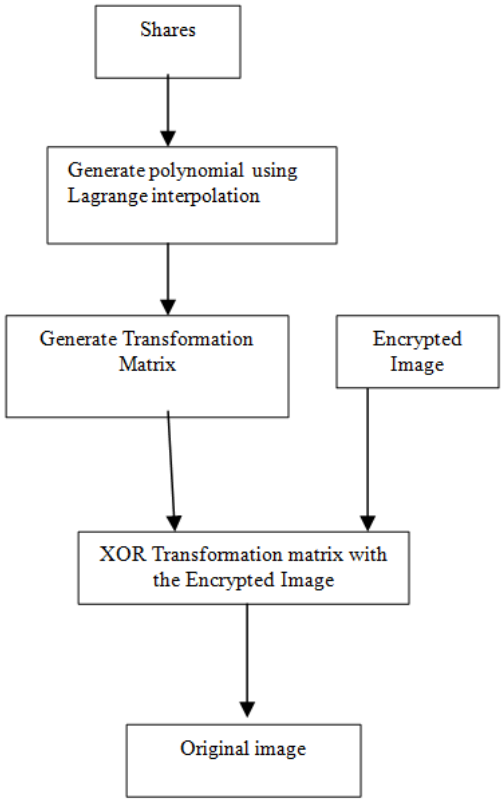

Figure 3. Decryption Process

7. Encryption Algorithm

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

8. Decryption Algorithm

1. Reconstruct the polynomial from “t” shares using Lagrange interpolation.
2. Construct the Transformation Matrix
3. XOR Transformation matrix with Encrypted Image matrix
4. Get the Original Image

9. Sample Images

Figure 4. Leena Image

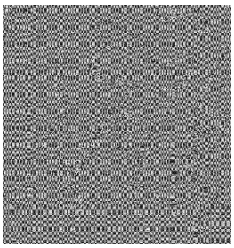

Figure 5. Encrypted Leena

Figure 6. Cameraman

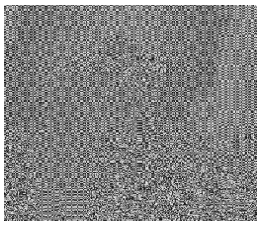

Figure 7. Encrypted Cameraman

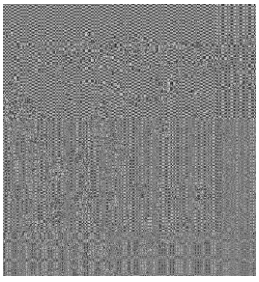

Figure 8. Gold hill

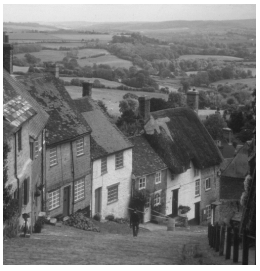

Figure 9. Encrypted Gold Hill

10. Analysis

10.1 Histogram Analysis

Histogram analysis is employed to illustrate its superior confusion and diffusion properties in the encrypted data. The histogram of the plain image cameraman is shown in Figure 10 and the histogram of the encrypted image is shown in Figure 11. Comparing the two histograms, we find that histogram of encrypted image is fairly uniform and is significantly different from that of the original image, and that the encrypted images transmitted do not provide any suspicion to the attacker, which can strongly resist statistical attacks.

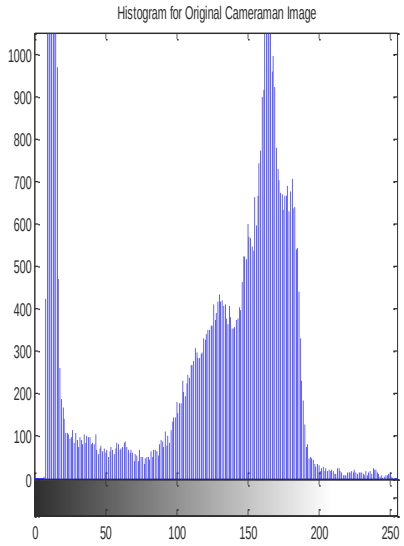

Figure 10. Histogram for Cameraman Original Image

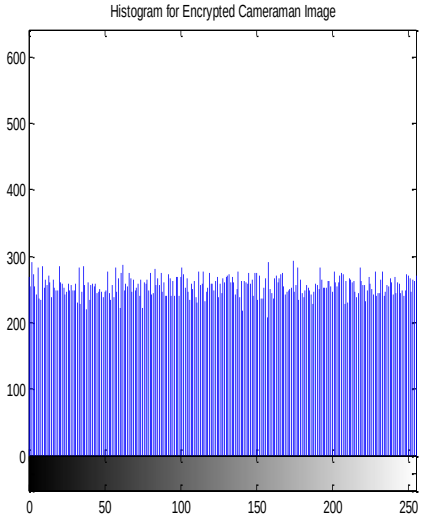

Figure 11. Histogram for Cameraman Encrypted Image

10.2 Encryption Quality Analysis

The quality of image encryption [12] may be determined as follows:

Let F and F' denote the original image and the encrypted image respectively each of size M * N pixels with L grey levels. F(x,y), F' (x,y) € {0, 1,….,L-1} are the grey levels of the images F and F' at position (x,y) ($0 \leq x \geq M-1$, $0 \leq Y \geq N-1$). Let $H_L(F)$ denote the number of occurrences of each grey level L in the original image F. Similarly , $H_L(F')$ denotes the number of occurrences of each grey level L in the encrypted image F'. The encryption

quality represents the average number of changes to each grey level L and is expressed mathematically as

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} | H_L(F') - H_L(F) |}{256}$$

The encryption Quality of this proposed algorithm is computed and is tabulated as follows.

Table 1. Encryption Quality Table

Image	Size	Encryption Quality
Leena	256 x 256	149.1953
Cameraman	256 x 256	252.6563
Gold Hill	512 x 512	713.7500

10.3. 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.

11. 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.

References

[1] H. Imai, G. Hanaoka, J. Shikata, A. Otsuka and A. C. Nascimento, "Cryptography with information theoretic Security", Information Theory Workshop, 2002, Proceedings of the IEEE, **(2002)** October 20-25.
[2] DingWei and QiDongxu, "Digital image transform, information hiding and camoufiage technique", Journal of computers, vol. 21, **(1998)** September, pp. 838 – 843.
[3] A. Shamir, "How to share a secret", Communication of the ACM, vol. 22, **(1979)**, pp. 612 - 613.
[4] M. Naor, "Visual Cryptography", In Proceeding of - Eurocrypt '94, **(1994)**, pp. 441–449.

[5] C. Zhenfu, "A threshold key escrow based on public key cryptosystem", Science in China (Series E), 200144, **(2001)** April, pp. 441–448.
[6] C. E. Shannon, "Communication Theory of secrecy systems", Bell System Technical Journal, vol. 28, **(1994)** April, pp. 656–715.
[7] B. Acharya, S. K. Patra and G. Panda, "A Novel Cryptosystem Using Matrix Transformation", Proceedings of SPIT-IEEE Colloquium & International Conference, vol. 4, **(2008)**, pp. 92 – 95.
[8] B. Acharya, G. S. Rath, S. K. Patra and S. K. Panigrahy, "Novel Methods of Generating Self Invertible Matrix for Hill Cipher Algorithm", International Journal of Security (CSS Journals), vol. 1, Issue 1, **(2007)**, pp. 14 – 21.
[9] H. J. Gao, Y. S. Zhang, S. Y. Liang, et. al., "A new Chaotic algorithm for Image Encryption", Chaos, Solutions and Fractals, vol. 29, **(2006)**, pp. 393-399.
[10] L. Bai, "A Reliable (k,n) Image secret sharing scheme", proceedings of the 2nd IEEE International Symposium on Dependable, Automatic and secure computing (DASC'06), ieee Computer Society, **(2006)**, pp. 1-6.
[11] C. Jeyamala, B. Subramanyan and G. S. Raman, "A Real time Image Encryption Techniques Based on Discrete Logarithms", L. M. Patnaik and Venugopal K. R. (Eds.), ICIP- 2010, (c) 1K International Publishing House Pvt. Ltd., New Delhi, **(2010)**, pp. 107-112.
[12] G. N. Krishnamurthy and V. Ramaswamy, "Encryption Quality Analysis and Security of CAST-128 Algorithm and its Modified Version Using Digital Images", International Journal of Network Security and its Applications (IJNSA), vol. 1, no. 1, **(2009)** April.

Authors

A.Kalai Selvi received her M.C.A. degree from Manonmanium Sundaranar University in 1993. She did her M.Phil Computer Science degree from Mother Theresa University in 2004. Presently she is working as an Associate Professor in S.T.Hindu College, Nagercoil since 1994. Her area of interest is "Multimedia Security". She is currently pursuing the Ph.D. degree.

M. Mohamed Sathik completed B.Sc.,and M.Sc., degrees from Department of Mathematics, M. Phill., from Department of Computer Science, M. Tech from Computer Science and IT ,M.S., from Department of Counseling and Psycho Therapy, and M.B.A degree from reputed institutions. He has 9 years working experience as a Coordinator for Computer Science Program, Directorate of Distance and Continuing Education, M. S. University. He served as Additional Coordinator in Indra Gandhi National Open University for four years. He headed the University Study Center for MCA Week End Course, Manonmaniam Sundaranar University for 9 years. He has been with the department of Computer Science, Sadakathullah Appa College for 23 years.Now he is working as a Associate Professor for the same department. He works in the field of Image Processing, specializing particularly in medical imaging. Dr. Mohamed Sathik M. guided 30 M.Phil Computer Science Scholors and guiding 14 Ph.D Computer Science Scholor from M.S.University, Tirunelveli, Barathiyar University, Coimbatore and Periyar Maniammai University, Tanjavur. He presented 12 papers in international conferences in image processing and presented 10 papers in national conferences. He published 5 papers in International Journals and 5 papers in proceedings with ISBN.