SELECTIVE ENCRYPTION OF IMAGE BY NUMBER MAZE TECHNIQUE

Santosh Mutnuru, Sweeti Kumari Sah and S. Y Pavan Kumar

Eastern Michigan University, USA

ABSTRACT

Due to enormous increase in the usage of computers and mobiles, today's world is currently flooded with huge volumes of data. This paper is primarily focused on multimedia data and how it can be protected from unwanted attacks. Sharing of multimedia data is easy and very efficient, it has been a customary practice to share multimedia data but there is no proper encryption technique to encrypt multimedia data. Sharing of multimedia data over unprotected networks using DCT algorithm and then applying selective encryption-based algorithm has never been adequately studied. This paper introduces a new selective encryption-based security system which will transfer data with protection even in unauthenticated network. Selective encryption-based security system will also minimize time during encryption process which there by achieves efficiency. The data in the image is transmitted over a network is discriminated using DCT transform and then it will be selectively encrypted using Number Puzzle technique, and thus provides security from unauthorized access. This paper discusses about numeric puzzle-based encryption technique and how it can achieve security and integrity for multimedia data over traditional encryption technique.

KEYWORDS

multimedia security, selective encryption; DCT compression; cipher image

1. INTRODUCTION

Multimedia communication plays a significant role in politics, economics, industrial sector, military, and entertainment. Any data which is transferred over the network with utmost ease will be susceptible to various kinds of attacks. To preserve security and integrity, data must be encrypted before its transmission or storage. Digital security attacks which include multimedia data attacks has an inclining affect from small privately-owned businesses to nonprofit organizations (Mutnuru, 2016).To generalize, digital security attacks can happen to any organization that uses digital information. Multimedia attacks vary from illegal access to information and/or monetary gain. Symantec's 2013 Internet Security Threat Report states that small organizations are not well prepared and cannot protect themselves for many external attackers (Symantec, 2013). The Symantec report reveals that in 2012, half of the targeted attacks were aimed at organizations that were less than 2,500 employees. These companies are often less careful in their cyber defenses and so make themselves low-difficulty intrusion targets, particularly for criminals

Encryption is the process of transforming the information into a form that only those it is intended for can read and process. There are different data encryption techniques widely available, but most of the available encryption algorithms are designed for textual data. Distinct types of data demand distinct aspects, and techniques to protect the confidentiality of data from unauthorized access. Usually image takes up more size when compared to text data because of which image demands more time for the encryption process. The textual encryption process

DOI:10.5121/ijcis.2020.10201

demands 100% exact results after decryption, whereas image decryption is acceptable with trivial distortion (Indrakanti & P.S.Avadhani, 2011). Various encryption schemes have been proposed for image encryption, [5,6] however in these schemes (fully encryption schemes) all data must be encrypted which generally takes more time, complex calculations and high memory consumption, hence these schemes are hard to use in real time applications.

Due to the intrinsic properties of visual information (like image, video) such as bulk data capacity, strong pixel correlation and high redundancy, lowers the encryption performance with respect to both time and memory. Selective (or soft or partial) encryption is an approach to reduce the computational resources for huge volumes of multimedia data in low power network as it protects the most visually important parts of an image or video representation (Som & Sen, 2013).

2. Existing System

Traditional multimedia (image and video) content protection schemes make use of fully layered encryption process in which the whole content is first compressed. Then, the compressed bit stream is entirely encrypted using a standard cipher (DES, AES, etc.) [3]. The specific characteristics of this kind of data (high-transmission rate with limited bandwidth) make standard encryption algorithms inadequate. This is due to the intrinsic properties of visual information such as bulk data capacity, strong pixel correlation and high redundancy which lower the encryption performance with respect to both time and memory (Droogenboeck & Benedit, 2002).

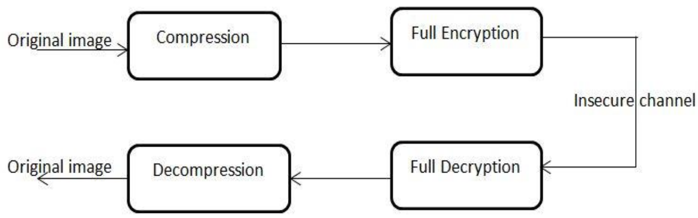

Fig. 1. Traditional full encryption approach

A. Problem Statement

Sharing of multimedia data over unprotected networks using DCT algorithm and then applying selective encryption-based algorithm has never been adequately studied. The objective of this paper is to take a multimedia image which will be applied through DCT algorithm and then through selective encryption-based algorithm which will finally be used to decrypt the image. The original image and reconstructed image should be identical. Also, several security analyses such as NPCR, UACI, MAE, PSNR etc. are to be carried out to prove the effectiveness, robustness, and security of proposed encryption algorithm over unprotected network.

3. The Proposed Method

The proposed method is based on the idea of decomposing the image into 8x8 blocks, which are then transformed from the spatial domain to frequency domain by applying DCT algorithm followed by quantization. Then, the DC coefficient and some selected coefficients related to the higher frequencies of the image block are selectively encrypted using a novel approach called Numeric Puzzle based encryption technique.

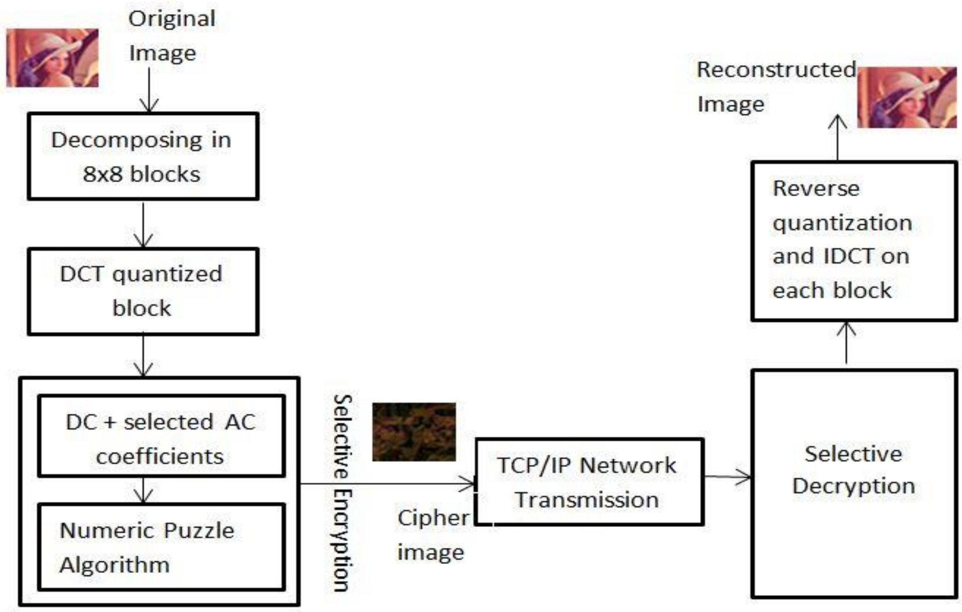

Fig. 2. Block diagram of proposed method

A. Sensitive part selection

A large majority of useful image contents change relatively slowly across images, i.e., it is unusual for intensity values to alter up and down several times in a small area within an image block. A translation of this fact into the spatial frequency domain implies, lower spatial frequency components contain more information than the high frequency components which usually correspond to less useful details and more unwanted noise. Humans are more immune to loss of higher spatial frequency components than loss of lower frequency components. For this reason, the idea of the proposed method is to take the DC and some AC coefficients of the lowest frequencies which must be encrypted selectively.

DC	AC	AC	AC	AC	AC		
AC	AC	AC	AC	AC			
AC	AC	AC	AC				
AC	AC	AC					
AC	AC						
AC							

Fig. 3. Selected parts to be encrypted from DCT matrix

B. Numeric Puzzle based image encryption algorithm

1

9	7	5	3	1
11	13	15	17	19
29	27	25	23	21
31	33	35	37	39
49	47	45	43	41
51	53	55	57	59

2

10	7	6	3	2
11	14	15	18	19
30	27	26	23	22
31	34	35	38	39
50	47	46	43	42
51	54	55	58	59

3

12	7	6	5	4
13	14	15	20	21
30	29	28	23	22
31	36	37	38	39
52	47	46	45	44
53	54	55	60	20

4

12	11	10	9	8
13	14	15	24	25
30	29	28	27	26
31	40	41	42	43
56	47	46	45	44
57	58	59	60	40

5

20	19	18	17	16
21	22	23	24	25
30	29	28	27	26
31	48	49	50	51
56	55	54	53	52
57	58	59	60	50

6

36	35	34	33	32
37	38	39	40	41
46	45	44	43	42
47	48	49	50	51
56	55	54	53	52
57	58	59	60	35

Fig. 4. Numeric Puzzle tables used for generating key

The technique uses 6 tables as shown in Figure 4.The principle behind using the table is as follows, let us consider a number 23 that has to be encrypted. Then we look for the tables consisting of this number. Here we can see table numbers 1, 2, 3 and 5 contain 23. So, our algorithm represents the number 23 as {1, 2, 3, and 4}. More detailed explanation is given in algorithm below.

The DC and selected AC coefficients from each 8X8 matrix are taken as pixel forms that will be applied to our proposed approach.

Steps in algorithm:

1. Read pixel values (R,G,B)

   Let us consider an image pixel having RGB values as:
   (184, 252, 207)

2. Perform modulo 60 (mod 60) and division by 60 on each pixel in order to get the remainders and quotients Q (R_q, G_q, B_q) and R (R_r, G_r, B_r)

Remainders	Quotients
184 % 60 = 4	184 / 60 = 3
252 % 60 = 12	252 / 60 = 4
207 % 60 = 27	207 / 60 = 3

   Hence, Q (3, 4, 3)
   R (4, 12, 27)
   [modulo 60 is performed to make the remainders and quotients values under 60 as tables values are under 60]

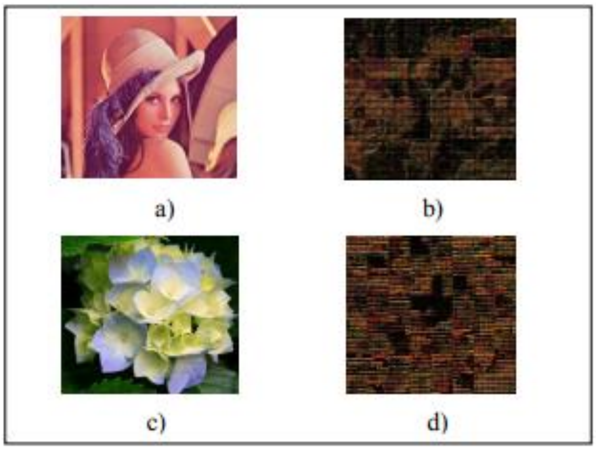

Fig. 5. (a) Original Lenna image (b) Selectively encrypted Lenna image (c) Original flower image (d) Selectively encrypted flower image

3.Scan from the table (maze) above, and list out all the tables for these Q and R values as (e.g., 3 present in table number 1 and 2).

Values	Table numbers
Q (3, 4, 3)	
3	1, 2
4	3
3	1,2
R (4, 12, 27)	
4	3
12	3,4
27	1,2,4,5

Q (3, 4, 3) → (1,2 3 1,2) – in quotient file
R (4, 12, 27) → (33,4 1,2,4,5) – in remainder file

4.Maintain quotient file and remainder file containing these values separated by delimiter for each next pixel(which will be concatenated and sent as key file).

Quotient file
1, 2, 3, 1, 2; …..
…. ; …..
(For next pixels)

Remainder file
3, 3, 4, 1, 2, 4, 5;
…. ; …..
(For next pixels)

5.Take the length of table numbers for both quotient and remainder (e.g., for table numbers 1,2,3,4 → length is 4)

Values	Table numbers	Length
Q (3, 4, 3)		
3	1, 2	2
4	3	1
3	1,2	2
R (4, 12, 27)		
4	3	1
12	3,4	2
27	1,2,4,5	4

Q_{len} = (2, 1, 2
R_{len} = (1, 2, 4)

6.Make these lengths as new pixels, keeping last pixel as 0.
The new pixel is thus, (124, 212, 0) [encrypted form]

C.Image decryption

Image decryption process at receiver side follows the reverse sequence of the image encryption. The flow starts with getting the keys and using Numeric puzzle algorithm in reverse order mode then following reverse quantization and Inverse Discrete Cosine Transformation (IDCT) to get the reconstructed image.

4. RESULTS AND ANALYSIS

Experiments are performed using different plain images of different pixel sizes to prove the validity of the proposed algorithm. Figures 5(b) and 5(d) are the output (cipher image) of our algorithm and the corresponding original images are shown in Figures 5(a) and 5(c).

Security Analysis

A good encryption procedure must be robust against all kinds of cryptanalytic, statistical analysis and brute-force attacks (GÜVENOĞLU&RAZBONYALI, 2019)[7]. Hence, the security analysis of the proposed image encryption scheme is done. Statistical analysis such as histogram analysis, Number of pixel change rate (NPCR) and Unified average change intensity (UACI), time and size analysis are performed to prove that the proposed cryptosystem is secure against the most common attacks.

A. Histogram Analysis

To demonstrate the strong resistance of our proposed algorithm to statistical attacks, test is carried out on the histogram of enciphered image. Various images of different sizes are selected, and their histograms are compared with their corresponding ciphered image. We can observe from one typical example shown in Figure 6 below that the histogram of original image contains larger spikes as compared to that of encrypted image. Thus, it is clear that histograms of enciphered image and original image bear no statistical resemblance to each other. Hence statistical attack on proposed image encryption procedure is difficult

.

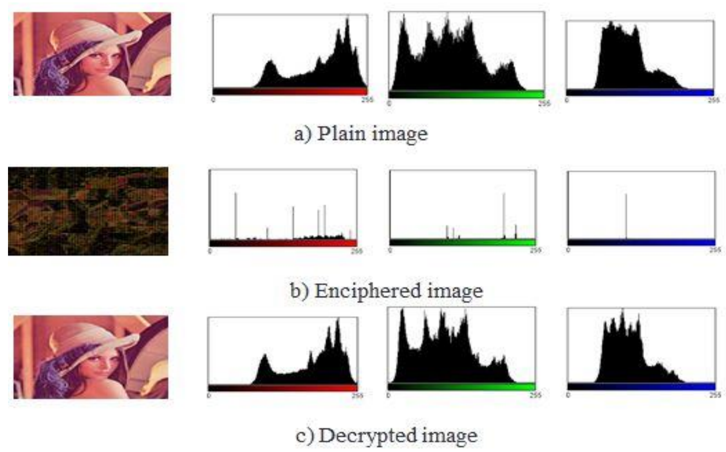

Fig. 6. Histogram analysis: (a), (b), and (c) respectively, shows a plain image, encrypted image, decrypted image and the corresponding histograms of red, green and blue channels.

Differential Attack Analysis

This is represented by the change produced on enciphered image by changing just one-pixel value in the plain image which depicts the quality of encryption algorithm. The parameters used are Number of pixel change rate (NPCR) and Unified average change intensity (UACI) [7] [8].

B. Number of pixel change rate (NPCR)

It is a common measure used to check the effect of one-pixel change on the entire image. This will indicate the percentage of different pixels between two images.

Let $C_1(i, j)$ and $C_2(i, j)$ be the pixels values of original and encrypted images, C_1 and C_2, at the i^{th} pixel row and j^{th} pixel column, respectively.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \qquad (1)$$

D(i, j): determined by $C_1(i, j)$ and $C_2(i, j)$, if $C_1(i, j) = C_2(i, j)$, then, $D(i, j) = 1$; otherwise, $D(i, j) = 0$. W and H: width and height of the image. Higher NPCR values are desired for ideal encryption schemes.

C.Unified average changing intensity (UACI)

A small change in plain image must cause significant change in cipher image. UACI is helpful to identify the average intensity of difference in pixels between the two images. For the plaintext image $C_1(i, j)$ and encrypted image $C_2(i, j)$ the equation (2) gives the mathematical expression for UACI.

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100 \qquad (2)$$

Table I. Performance Analysis With Npcr And Uaci Values

Image	*Size*	*NPCR (%)*	*UACI (%)*
Lenna	512×512	99.929	45.853
flower	464×400	93.555	38.137
pepper	256×256	99.146	31.648
ChestXray	512×512	95.553	52.189

D. Time and Size Analysis

Along with security consideration, execution speed of the algorithm is an important factor for a good encryption algorithm. The time analysis has been done on Intel Core i5 with 4GB RAM computer for several images of different sizes and is shown in Table II. Also, as the process follows quantized DCT transformation the size of original image, cipher image and decrypted image on disk are reduced with significant saving of memory which is shown in Table III.

Table II. Average Encryption/ Decryption Speed Of Algorithm

Image	***Encryption time (ms)***	***Decryption time (ms)***
Lenna	2381	171
Flower	2032	125
Pepper	844	47
ChestXray	2725	204

Table III. Size Of Images On Disk At Various Stages

Image	**Size on disk (KB)**		
	Original	***After encryption***	***After decryption***
Lenna	462	78.7	26.3
flower	76.8	72.3	22.6
pepper	24.0	22.1	7.6
ChestXray	110	69.4	25.4

E. Mean absolute error (MAE)

It gives the measure of how close predictions are to the eventual outcomes. The larger values of MAE are considered better for image security.

$$MAE = \frac{1}{W \times H} \sum_{i} \sum_{j} | C_1(i,j) - C_2(i,j)| \tag{3}$$

F. Peak signal to noise ratio (PSNR)

Peak Signal-to-Noise Ratio is the ratio between the original image and the encrypted image measured in decibel. It depicts the measure of reconstruction of the encrypted image. The higher the PSNR, the closer the encrypted image is to the original. In general, a higher PSNR value should correlate to a higher quality image. For good encryption scheme the PSNR should be as low as possible.

$$PSNR = 10.\log_{10}\frac{(255)^2}{\frac{1}{W \times H}\sum_0^{W-1}\sum_0^{H-1}[C_1(i,j) - C_2(i,j)]^2} \quad (4)$$

TABLE IV. Performance Analysis With Psnr And Mae Values

Image	***PSNR (db)***	***MAE***
Lenna	5.934	101.519
Flower	7.406	80.231
Pepper	10.055	70.103
ChestXray	5.169	124.394

5. CONCLUSION

This paper shows successful implementation of selective image encryption using DCT transform and Numeric puzzle algorithm, a mechanism which provides high level of securityover unprotected network. The algorithm encrypts DC coefficients and some AC coefficients from each 8x8 DCT matrix. The image has been encrypted and decrypted successfully and has retained its original format thus by ensuring confidentiality, integrity, and availability traits. Several security analyses such as NPCR, UACI, MAE, PSNR etc. are carried out which proves the effectiveness, robustness, and security of proposed encryption algorithm.

REFERENCES

[1] Sesha Pallavi Indrakanti and P.S.Avadhani, “Permutation based image encryption technique,” International Journal of Computer Applications, vol. 28– No.8, August 2011, pp. 45-47.

[2] Sukalyan Som & Sayani Sen, (2013) “A Non-adaptive Partial Encryption of Grayscale Images based on Chaos”, Procedia Technology, vol. 10, pp. 663-671.

[3] Mutnuru, S., PhD. (2016). The role of internal controls on employees' engagement in small organizations. JournalofBusinessStudiesQuarterly,7(4),102-114.Retrievedfrom http://search.proquest.com/docview/1807472170?accountid=35812

[4] P.R. Sankpal, P.A. Vijaya, "Image Encryption Using Chaotic Maps: A Survey", 2014 Fifth International Conference on Signal and Image Processing (ICSIP), Karnataka (India), pp. 102-107, 8-10 Jan. 2014. DOI:10.1109/ICSIP.2014.80

[5] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap and Amit Kumar Mishra, “Text and Image Encryption Decryption Using Advanced Encryption Standard,” IJETTCS, vol. 3, June 2014, pp. 118-126.

[6] GÜVENOĞLU, E , RAZBONYALI, C . (2019). The Creation of Maze in Order to Hide Data, and the Proposal of Method Based on AES Data Encryption Algorithm. El-Cezeri Journal of Science and Engineering , 6 (3) , 668-680 . DOI: 10.31202/ecjse.571030

[7] Deepti C. Gavankar, C. Madhumita, and Suhas J. Lawand, “Secure Real Time Remote Video Monitoring Using Selective Encryption”, IEEE paper, 2012, pp. 453-457.

[8] Tieyu Zhao, Qiwen Ran & Yingying Chi, (2015) “Image encryption based on nonlinear encryption system and public-key cryptography”, Optics Communications, vol 338, pp. 64-72.

[9] A. Alfalou, C. Brosseau & N. Abdallah, (2015) “Simultaneous compression and encryption of color video images”, Optics Communications, vol 338, pp. 371-379.

[10] R. Gupta, A. Aggarwal & S.K. Pal, “Design and Analysis of New Shuffle Encryption Schemes for Multimedia”, Defence Science Journal, Vol. 62, No. 3, May 2012, pp.159-166.

[11] P. Maggo, Dr R.S. Chhillar, “Security of Multimedia Data: A Review Paper on various Image Security Algorithms”, National Conference on Advanced Computing Technologies, Vol. 2, March 2013,pp. 852-857.

[12] Pavithra. C and Vinod. B. Durdi, “Analization and Comparison of Selective Encryption Algorithms with Full Encryption for Wireless Networks”, International Journal of Engineering Trends and Technology (IJETT), vol. 4 Issue 5,May 2013.

[13] Droogenbroeck, Marc & Benedett, Raphal. (2002). Techniques For A Selective Encryption Of Uncompressed And Compressed images.