Secured Image Compression using Wavelet Transform

G. Suseela*, Niharika Kumari and Y. Asnath Victy Phamila

VIT University, Chennai Campus, Chennai – 600127, Tamil Nadu, India;
suseelarajeshkanna@gmail.com, niharica.purvi@gmail.com, phamila@outlook.com

Abstract

Objective: Image Compression is to shrink insignificance and redundancy of the image data and it is obligatory for efficient transmission and storage of images. Image data are self-descriptive and contains sensitive information, yet partial data will convey more information. Hence robust security mechanisms are required for defending and privacy protection of image data. A robust secured image compression scheme has been proposed in this paper. Methods: In this work two levels of security have been accomplished to improve the robustness of the encryption system. Torus Automorphism and Rubik’s cube principle are used for pixel scrambling and shuffling along with adaptive DWT based image compression. Findings: Extracting greatest image quality at a given bit-rate or compression ratio is the main goal of Image Compression. Experimental results have shown that the proposed system of secured image compression offers compression ratio of 97% and a bit rate of 0.25bpp and the scheme is highly robust with respect to the security parameters such as UACI (Unified Average Changing Intensity) and NPCR (Number of Pixels Change Rate). Application: The proposed scheme is highly suitable for small hand held wireless communication gadgets such as mobile phones to upload/download on/from Internet, where fast and efficient on the fly image encryption and transmission are required.

Keywords: Compression, DWT, Encryption, Rubik’s Cube, Torus Automorphism

1. Introduction

Image contains huge volume of pixel data with redundancies. Compression takes out the redundancies. Image compression reduces the size of an image file without affecting major loss to the quality of the image by retaining necessary pixel data. Thus compression allows efficient utilization of time, memory and bandwidth in digital image communication. The compression algorithm may be of lossless or of lossy type. The lossless compression schemes can be used in systems where a very high image quality required and loss of data is intolerable. Lossless compression is favoured for authentication grits and useful for image archiving as in the storage of medical images, comics, technical diagrams etc. Lossy compression schemes allow high compression ratio with acceptable image quality. In lossy compression, the original data cannot be accurately reconstructed from the compressed data. The reason is the redundant pixel data in an image are discarded without changing the appearance of the image to a great extent. Lossy methods are generally proper for natural images such as photographed pictures used in applications where slight loss of accuracy is acceptable to attain a significant reduction in bit rate. These are useful in applications such as videoconferencing, broadcast television, etc., in which a certain loss of quality is acceptable for increased compression performance. The compressed bit streams are further entropy coded.

When numerical or alphanumerical data are trapped the attackers have to rightly interpret them to get the information part since they will not convey any meaning. When the image is cracked by interveners during transmission, it will reveal more information because images are self-descriptive and hence sensitive. One of the main goals that ought to be accomplished during the transmission of images over the communication network is security. Image cryptography is the technique which is widely used for secure transmission of image data. The image encryption algorithms aim at converting the original image into unreadable cipher image. The encryption algorithms are categorized into several types.
Secured Image Compression using Wavelet Transform

Such that substitution, permutation/ transposition etc. Substitution schemes modify the pixel values of image whereas permutation based schemes shamble the pixel positions of image based on predefined procedures. One or two of these methods can be combined for increased robustness. The encryption algorithms also classified into two types such as symmetric and asymmetric based on key distribution policy. The symmetric encryption technique will encrypt the image with a secret key and at decryption stage the authorized person who holds the same key can recover the information.

2. Related Work

There are many image encryption algorithms are available in the recent literature. They are based on Blowfish algorithm, chaotic and logistic maps, pixel swapping based on permutation schemes, pixel scrambling, and etc., Rubik’s cube scrambling have been adapted by many researchers. In Rubik cubes based encryption the key is generated randomly with length of image size and encryption algorithm is applied on the entire image involving heavy computational load making adaptability impossible in low power embedded systems like mobile devices, sensor devices. The proposed system is based on block based image encryption along with compression. In the proposed system the encryption key size is n, where n refers block size, for demonstration the assumed value of n is 8. In Rubik cubes after pixel scrambling bit wise XOR is applied over the image with the same keys. To have second level of security in proposed system Torus Automorphism pixel swapping is used. Any compression algorithm follows a three step chained process i.e., (Transformation-Quantization-Entropy coding). But the proposed secured compression follows yet another three step process i.e., (Transformation-Encryption-Entropy coding). Wavelet transform has been chosen for its long list of advantages especially the image quality is very good at low bitrate.

The transformed - encrypted image is further entropy coded using the prefix based Huffman coding.

3. Proposed System

As a first step the original image is pre-processed. To follow the three steps of the chained process the image is wavelet transformed. The LL (Approximation) band alone selected for encryption. Encryption is the second step of the chained process; here two different image encryption schemes are used. Torus Automorphism technique is applied to the entire transformed LL band for pixel shuffling. Second level of encryption is done using Rubik’s cube pixel scrambling. Third step of the chained process is entropy coding; Huffman coding is used to generate the compressed bit stream. The proposed system architecture is illustrated in Figure 1.

Figure 1. Proposed system architecture.

3.1 Discrete Wavelet Transformation

The proposed secured compression algorithm uses wavelet transformation. DWT decomposes the image into several sub bands that is, HH, HL, LH, and LL as shown in Figure 2. The LL band contains most significant pixel data of the image, such that approximated version of the original image. Only the LL band is considered in our system for secured compression.
3.2 Torus Automorphism

Torus Automorphism (TA) is a dynamic system which changes its state with respect to time. TA is based on permutation in two dimensional spaces like matrices\(^1\). It is used for pixel shuffling within the image in image encryption system. The shuffled new pixel positions are computed using the transform function as shown below. Where \(x\) and \(y\) are the new pixel positions and \(a\), \(b\) are the original pixel positions. The result of the TA is an obfuscated image.

\[
\begin{align*}
    x &= 1 \cdot a + 1 \cdot b \\
    y &= 1 \cdot a + 2 \cdot b
\end{align*}
\]

3.3 Rubik’s Cube Scrambling

Rubik’s cube principle is applied in image encryption for pixel scrambling\(^1\). The Rubik’s cube algorithm uses two secret keys of length equal to one dimensional size of the original image. One key is applied for scramble the row and another key is for scramble the column. The proposed system follows the block level pixel scrambling; the assumed block size is 8x8. The Secret key size is reduced to a length of one dimensional size of the block i.e., 8. Rubik’s cube encryption and decryption procedure\(^1\) is depicted as in Figure 3.

![Flow Diagram of Rubik’s Cube Algorithm.](image)

3.3.1 Rubik’s Cube Encryption

1. Read any gray scale image of size \(M \times N\) as “Input Image”. Input Image β image read of size \(M \times N\)
2. Generate two random vectors “\(V_{row}\)” of length \(M\) and “\(V_{column}\)” of length \(N\) respectively.
3. For every row “\(i\)” of image
   3.1 Calculate the summation of all pixels in the row “\(i\)” and store in \(sum\_row\)
   3.2 Calculate modulo 2 of summation of each row and store in \(mod\_row\)
   3.3 If \(mod\_row=0\) → right circular shift will be done on \(i^{th}\) column.
   3.4 Else → left circular shift will be done on \(i^{th}\) column
4. Store this Image as row_scr
5. For every column “\(j\)” of image. [Input will be row_scr]
   5.1 Calculate the summation of all elements in the column “\(i\)” and store in \(sum\_col\)
   5.2 Compute modulo 2 of sum of each col and store in \(mod\_col\)
   5.3 If modulo=0 → upper circular shift will be done on \(j^{th}\) column.
   5.4 Else → Down circular shift will be done on \(j^{th}\) column
6. Store this Image in matrix col_scr
7. Then Bitwise XOR will be applied on Scrambled Image as Img_encr

3.3.2 Rubik’s Cube Decryption

1. Bitwise XOR will be applied on Encrypted Image.[Input will be Img_encr]
2. For every column “\(j\)” of image. [Input will be Img_bxor]
   2.1 Calculate the summation of elements in the column “\(i\)” and store in \(sum\_dcol\)
   2.2 Calculate modulo of 2 sum of each col and store in \(mod\_dcol\)
   2.3 If modulo=1 → Up circular shift will be done on \(j^{th}\) column.
   2.4 Else → Down circular shift will be done on \(j^{th}\) column
3. Then store this Image in one matrix. col_dscr
4. For every row “\(i\)” of image[Input will be col_dscr]
   4.1 Calculate the summation of all pixels in the row “\(i\)” and store in \(sum\_drow\)
   4.2 Calculate modulo of 2 sum of each row and store in \(mod\_drow\)
   4.3 If modulo=0 → right circular shift will be done on \(i^{th}\) column
   4.4 Else → left circular shift will be done on \(i^{th}\) column
5. Then store this Image in one matrix. Img_dec

4. Experimental Results and Discussion

The above proposed system is implemented in MatLab
2013a version. Experiments have been repeated for various test images of size 512 x 512. Results of images including Lena, Barbara, Baboon, Girl face and peppers are presented in Figure 4.

Figure 4. a) Original, encrypted and decrypted Lena Image b) Original, encrypted and decrypted Baboon Image. c) Original, encrypted and decrypted Barbara Image d) Original, encrypted and decrypted peppers Image e) Original, encrypted and decrypted Girl face Image.

5. Performance Analysis

The performance analysis is twofold in the proposed system. First the performance of encryption algorithm is analysed and secondly the performance of compression algorithm is analysed. The strength of encryption algorithm against various attacks is decided by two parameters. They are UACI (Unified Average Changing Intensity) and NPCR (Number of Pixels Change Rate). The performance of compression algorithm is determined by compression ratio and quality of compressed image is determined two error metrics namely Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

5.1 NPCR

It is a measure used to check the rate of changing the pixels of the encrypted image, when only one pixel is get changed over the whole input image. This is because as per key sensitivity analysis when one pixel is changed in the encrypted image, the encryption system should harvest a totally different encrypted image. NPCR in percentage is mathematically defined as,

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100}{MN}$$

where, M is the number of rows and N is the number of columns of pixel matrix. The values of the matrix E is decided by the following condition, if $I_n(i, j) = I_{enc}(i, j)$ then $E(i, j) = 0$ else $E(i, j) = 1$, where $I_n$ is the input image and $I_{enc}$ is the encrypted image.

5.2 UACI

It is used to recognize the difference in average intensity between the input Image pixels and Encrypted Image pixels. Mathematical expression for UACI is as

$$UACI = \left( \frac{100}{255} \right) \times \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| I_o(i, j) - I_{enc}(i, j) \right|$$

where, $I_o$ is the input image and $I_{enc}$ is the encrypted image.

5.3 Compression Ratio

It is defined as ratio between the sizes of compressed and uncompressed images.

5.4 Mean Square Error

The MSE equates the increasing squared error between the original image and the compressed one.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I_o(i, j) - I(i, j))^2$$

where, $I_{input}$ is the original image pixel matrix and $I_{comp}$
is the compressed image pixel matrix.

As much lower the value of MSE means that the higher image quality will be. PSNR while the PSNR represents the amount of error relative to the peak pixel value. For a gray scale image, the peak value is 255.

\[ PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right) \]

Table 1 demonstrates the experimental results of the proposed system. The compression ratio achieved by the proposed system is 1:32. For comparison purpose the experiments have been done with two different schemes. Scheme 1 is only with encryption using Rubik’s cube scrambling without compression procedure. Our proposed system compression using DWT and two levels security algorithm is experimented in Scheme 2. Table 2 and Table 3 represent the UCAI, NPCR values of scheme 1 and Scheme 2. From Tables 2 and 3, it is well understood that the proposed system robust and stable against differential attacks even after compression.

Table 1. NPCR, UACI and PSNR of the proposed system

| Images       | NPCR  | UACI  | PSNR |
|--------------|-------|-------|------|
| Lena         | 99.84 | 36.87 | 47.78|
| Baboon       | 99.82 | 36.12 | 48.38|
| Girl face    | 99.79 | 33.93 | 47.39|
| Peppers      | 99.84 | 37.38 | 48.00|
| Barbara      | 99.90 | 40.37 | 42.03|

Table 2. NPCR %

| Algorithm | Lena  | Baboon | Girl face | Barbara | Peppers |
|-----------|-------|--------|-----------|---------|---------|
| Scheme[1] | 99.73 | 99.68  | 99.87     | 99.72   | 99.81   |
| Scheme[2] | 99.84 | 99.82  | 99.79     | 99.76   | 99.77   |

Table 3. UACI %

| Algorithm | Lena  | Baboon | Girl face | Barbara | Peppers |
|-----------|-------|--------|-----------|---------|---------|
| Scheme[1] | 31.84 | 30.06  | 35.45     | 31.75   | 36.21   |
| Scheme[2] | 36.87 | 36.12  | 33.93     | 31.11   | 32.97   |

6. Conclusion

In this communication, an image encryption algorithm is proposed along with compression. There are two techniques used for encryption, first encryption technique is Torus Automorphism and the second technique is established on the Rubik’s cube pixel scrambling to commute pixels of the image. To baffle the correlation between input image and ciphered image, the Bitwise XOR operation is executed on scrambled image using a key. For compression DWT is used with Huffman Coding. The secured image compression scheme follows three step chained process as: Transformation-Encryption-Entropy coding. Experiments results were analysed which rigs the robustness of the proposed scheme against different categories of attacks. Performance assessment of compression technique shows 97% compression (bitrate of 0.25bpp) with acceptable image quality and security. The scheme proves to be highly appropriate for small hand held communication gadgets such as mobile phones to upload/download on/from Internet, where fast, robust and efficient on the fly image encryption and transmission are required.

6. References

1. Zain Eldin H, Elhosseini MA, Ali HA. Image compression algorithms in wireless multimedia sensor networks: A survey. Ain Shams Engineering Journal. 2015 Jun 30; 6(2):481–90.
2. Abraham L, Daniel N. Secure image encryption algorithms: A review. International Journal of Scientific and Technology. 2013; 2(4):186–9.
3. Singh P, Singh K. Image encryption and decryption using blowfish algorithm in Matlab. International Journal of Scientific and Engineering Research. 2013 Jul; 4(7):150–4.
4. Wu Y, Yang G, Jin H, Noonan JP. Image encryption using the two-dimensional logistic chaotic map. Journal of Electronic Imaging. 2012 Jan; 22(3):151–61.
5. Lu B, Zhao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solutions and Fractals. 2004 Jul; 21(3):749–61.
6. Habibpour L, Yousefi S, Lighvan MZ, Aghdasi HS. 3D Chaos-based image encryption acceleration by using GPU. Indian Journal of Science and Technology. 2016 Feb 4; 9(6):1–6. DOI: 10.17485/ijst/2016/v9i6/72651.
7. Jolfaei A, Wu WX, Muthukumarasamy V. On the security of permutation-only image encryption schemes. IEEE Transactions on Information Forensics and Security. 2016 Feb; 11(2):235–46.
8. Indrakanti SP, Avadhani PS. Permutation based image encryption technique. International Journal of Computer Applications. 2011 Aug; 28(8):45–7.
9. Meenakshi P, Manivannan D. An efficient three layer image security scheme using 3D Arnold Cat Map and Sudoku Matrix. Indian Journal of Science and Technology. 2015 Jul; 8(16):1–6. DOI: 10.17485/ijst/2015/v8i16/63545.
10. Loukhaoukha K, Chouinard JY, Berdai A. A secure im-
Secured Image Compression using Wavelet Transform

11. Gomathi T, Shivakumar BL. Multistage image encryption using Rubik’s Cube for secured image transmission. International Journal of Advanced Research in Computer Science. 2015 Jul/Aug; 6(6):54–8.
12. Suseela G, Phamila AVY. Visual sensor networks: Critical infrastructure protection. Combating Security Breaches and Criminal Activity in the Digital Sphere; 2016 Jun 9. p. 263–82.
13. Duran-Faundez C, Lecuire V, Lepage F. Tiny block-size coding for energy-efficient image compression and communication in wireless camera sensor networks. Signal Processing: Image Communication. 2011 Oct; 26(8):466–81.
14. Phamila AVY, Amutha R. Energy-efficient low bit rate image compression in wavelet domain for wireless image sensor networks. Electronics Letters. 2015 May; 51(11):824–6.
15. Ganesh SS, Mohanaprasad K, Karuna Y. Object identification using wavelet transform. Indian Journal of Science and Technology. 2016 Feb 9, 9(5):1–7. DOI: 10.17485/ijst/2016/v9i5/87187.
16. Nasri M, Helali A, Sghaier H, Maaref H. Adaptive image compression technique for wireless sensor networks. Computers and Electrical Engineering. 2011 Sep; 37(5):798–810.
17. SIBI Image Database [Internet]. Available from: http://sipi.usc.edu/database/database.
18. Ahmad J, Ahmed F. Efficiency analysis and security evaluation of image encryption schemes. International Journal of Video Processing and Network Security. 2000; 54(11):109–33.