International Journal of Current Trends in Engineering & Technology
Received 3 Dec., 2018, Revised Received, 20 Dec., 2018, Accepted 23 Dec., 2018, Available online 25 Dec., 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 06 (November- December, 2018)

ANALYSIS OF A NOVEL APPROACH FOR LOSSLESS DIGITAL IMAGE TRANSMISSION BY CRYPTOGRAPHY AND WATERMARKING

Vinay Gupta, Rahul Dhakad
Electronic and Communication Department RDIST, Bhopal
Rahuldhakad12345@gmail.com
+91, 9575950319

Abstract— *now a day's users share their private information through the network. People use internet banking on line shopping and billing, data security is the major concern for all users. Emerging changes of technology and dependability on digital technology creates a huge demand of cryptography; which is the back bone of communication system. The main motivation behind this dissertation work is the advancement of cryptography in the field of Image Processing, Image Processing is new and promising area of research and cryptography algorithm for image has lot of scope to conduct research. The objective of this research is to access need of new cryptography algorithm and provide a secure image transmission in network by generating a new cryptography algorithm and retrieve a secure, lossless image at receiving end. Proposed work will compare the result with other algorithms to judge the effectiveness of research work.*

Keywords: - Digital Image, Lossless Image, Cryptography, Watermarking.

1. INTRODUCTION

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. In a (8-bit) grey scale image each picture element has an assigned intensity that ranges from 0 to 255. A grey scale image is what people normally call a black and white image, but the name emphasizes that such an image will also include many shades of grey. Some grey scale images have more grey scales, for instance 16 bit = 65536 grey scales. In principle three grey scale images can be combined to form an image with 281,474,976,710,656 grey scales. There are two general groups of 'images': vector graphics (or line art) and bitmaps (pixel-based or 'images'). Some of the most common file formats are:

- GIF (Graphics Interchange Format) - An 8-bit (256 color), non-destructively compressed bitmap format. Mostly used for web.
- JPEG (Joint Photographic Experts Group) - Avery efficient (i.e. much information per byte) destructively compressed 24 bit (16 million colors) bitmap format. Widely used, especially for web and Internet (bandwidth-limited).
- TIFF (Tagged Image File Format) - The standard 24 bit publication bitmap format. Compresses non-destructively with, for instance, Lempel-Ziv-Welch (LZW) compression.
- PS- (Post Script) a standard vector format. Has numerous sub-standards and can be difficult to transport across platforms and operating systems.
- PSD - A dedicated Photoshop format that keeps all the information in an image including all the layers.
- Colors- For image transmission, the two main color spaces are RGB and CMYK.

The RGB color model relates very closely to the way we perceive color, Where R is red, G is green, and B is Blue. RGB uses additive color mixing and is the basic color model used in television or any other medium that projects color with light. It is the basic color model used in computers and for web graphics, but it cannot be used for print production.

2. Type of Cryptography Algorithm

There are generally two types of cryptography

(a) Symmetric Key Cryptography: Symmetric-key algorithms are a type of algorithms for cryptography that use a similar Cryptologic key for each plaintext and secret writing of ciphertext. The keys could also be identified or there could also be a straightforward transformation to travel between the 2 keys. The keys, in applying, represent a shared secret between 2 or additional parts that may be accustomed maintain a non-public data link. Symmetric-key encoding will use either stream ciphers or block ciphers.

- Stream ciphers encode the digits (typically bits) of a message one at a time.
- Block ciphers take a variety of bits and encode them as one unit, artifact the plain text in order that it's a multiple of the block size. Blocks of

International Journal of Current Trends in Engineering & Technology
Received 3 Dec., 2018, Revised Received, 20 Dec., 2018, Accepted 23 Dec., 2018, Available online 25 Dec., 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 06 (November- December, 2018)

sixty four bits are usually used. The Advanced encoding customary (AES) algorithmic program approved by the Authorities in Gregorian calendar month 2001 uses 128-bit blocks.

- It is feasible to encode while not mistreatment any mounted algorithmic program. Non-algorithmic Encryption.

(b) Asymmetric Key Cryptography: Asymmetric key encoding uses totally different keys for encoding and secret writing. These 2 keys square measures mathematically connected and that they type a key try. One among these 2 keys ought to be unbroken non-public, referred to as a private - key, and therefore the difference will be created public (it will even be sent in the mail), referred to as public-key. Therefore this can be additionally referred to as Public Key encoding. A private secret's generally used for encrypting the message-digest; in such Associate in nursing application private-key formula is termed message-digest encoding formula. A public secret's generally used for encrypting the secret-key; in such an application private-key formula is termed key encoding formula.

Different Media for Watermarking

Watermarking can be done for different media. Different techniques are applied for each of them. They are described as follows.

Text Watermarking: It can be done at the printout level or the semantic level of the text document.

At the printout level the information can be encoded in the way the text lines or words are separated. In this case the watermark survives even after photocopying At the Semantic level we use equivalences between words or expressions. In this case raw text files are provided.

Image Watermarking: It can be done in the spatial or frequency domain. The watermark is added to the image in this case and it can be visible or invisible. The techniques explained above are applied to image watermarking.

Audio Watermarking: In audio watermarking time and frequency masking properties of human ear are used to conceal the watermark and make it compressed data. All image watermarking techniques are equally applicable for video. In addition to the spatial domain in images we can also exploit the presence of temporal domain in video.

Software Watermarking: In this technique some digital data (watermark) embedded in a large digital media file (cover text).Here the data structure represents watermark where as the cover text is a software program. The requirement is that the watermarked program must be able to sustain various attacks on the watermark that it contains. Software watermarking protects intellectual copyright by discouraging software pirates from copying and reselling software.

3. Problem Statement

Earlier algorithm like AES (Advanced Encryption Standard), DES (Data Encryption Standard) and RSA is not being used due to losses. There are many algorithms used for text data but availability of image algorithm is very less as compare to text algorithm so there is a requirement of new cryptography algorithm for secure and lossless multimedia (Text, Image, voice) data transmission.

4. Proposed Algorithm for Watermarking

AES is the most recent and potential, the most secure encryption method published by NIST. It is a symmetric key block cipher that was designed to be a significant improvement over 3-DES/DES. AES is quick in each software package and hardware.

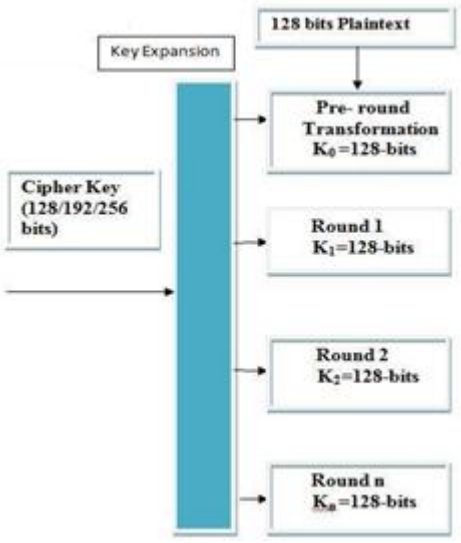


Figure 1 AES round bits representation

In contrast to its precursor DES, AES does not use a Feistel network. AES could be a variant of Rijndael algorithm that contains a block of key size of 128 bits, and a size of key 128, 192, or 256 bits. In contrast, the Rijndael algorithm specification with a block and key sizes that will be any multiple of thirty two bits, each

International Journal of Current Trends in Engineering & Technology
Received 3 Dec., 2018, Revised Received, 20 Dec., 2018, Accepted 23 Dec., 2018, Available online 25 Dec., 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 06 (November- December, 2018)

with a minimum of 128 and a most of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, though some versions of Rijndael algorithm have a bigger block size and have extra columns within the state. The key size used for the Associate in computes AES cipher specifies the quantity of repetitions of transformation rounds that convert the input, referred to as the plaintext, into the ultimate output, referred to as the cipher text.

Proposed Algorithm for Watermarking (DWPT)

Watermark embedding and extraction

The main concept of digital watermark embedding process is shown below in the figure3

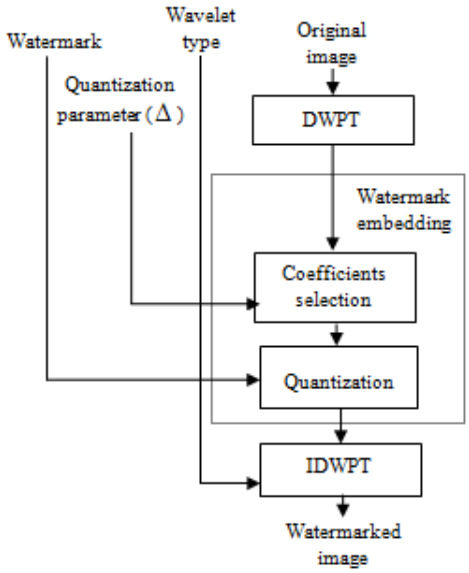


Figure 2 Watermark Embedding Procedure

The main concept of watermark embedding process a watermark, which is random binary string, is embedded into discrete wavelet domain by using the discrete wavelet packet transform (DWPT) during the embedding process. This watermark is only known by the owner. Moreover, the watermark is embedded into selected coefficients of selected blocks by quantizing the coefficients with a specified user defined quantization parameter Δ. The main steps of the embedding process are as follows:

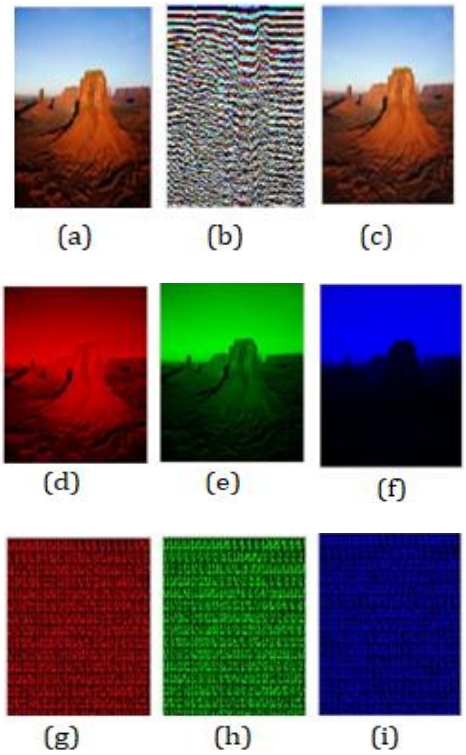
1. Discrete wavelet packet transform (DWPT) is applied. A fully wavelet packet structure, same as shown in Figure 2, is used in our proposed method. An m scale, full wavelet packet decomposition is applied thus 2^2m blocks appear during the embedding process.
2. The largest absolute value of coefficients will be selected. The amount of the selected coefficients is according to the row size of the selected blocks. In our method, one row of largest absolute value of coefficients will be selected. One block embeds one watermark bit. In this case, all m-level horizontal blocks are selected. The coefficients, which are embedded watermark bits, are selected among these blocks by using the quantization parameter Δ.
3. Each of the selected coefficients c will be divided by Δ. The equation is as follows:

$$Q(c) = \begin{cases} 1, & \text{if } \frac{c}{\Delta} = k \quad k = k \pm 1, k \pm 3, k \pm 5 \ldots\ldots \\ 0, & \text{if } \frac{c}{\Delta} = k \quad k = k \pm 2, k \pm 4, k \pm 6 \ldots\ldots \end{cases}$$

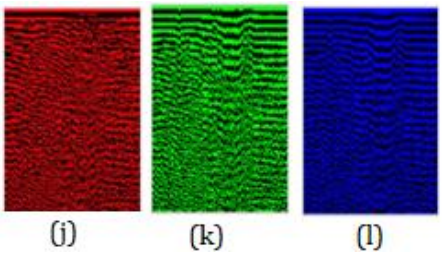
4. Compare each watermark bit m W with Q(c) of each selected coefficients in the corresponding block. If Q(c) = Wm, the coefficient c remains unchanged. If Q(c) ≠ Wm, the coefficient c = c + Δ.
5. Inverse discrete wavelet packet transform (IDWPT) is applied after all watermark bits are embedded. Finally, a watermarked image appears.

5. Result & Analysis

Result of Cryptography



International Journal of Current Trends in Engineering & Technology
Received 3 Dec., 2018, Revised Received, 20 Dec., 2018, Accepted 23 Dec., 2018, Available online 25 Dec., 2018
www.ijctet.org, ISSN: 2395-3152
Volume: 04, Issue: 06 (November- December, 2018)



3 (a)Original Image, (b)Encrypted image using DCT, (c) Decrypted image, (d)Red color component, (e)Green color component, (f)Blue color Component, (g)Encrypted red component, (h)Encrypted green component, (I)Encrypted blue component, (j)Encrypted red using DCT (k)Encrypted green using DCT, (l)Encrypted blue using DCT

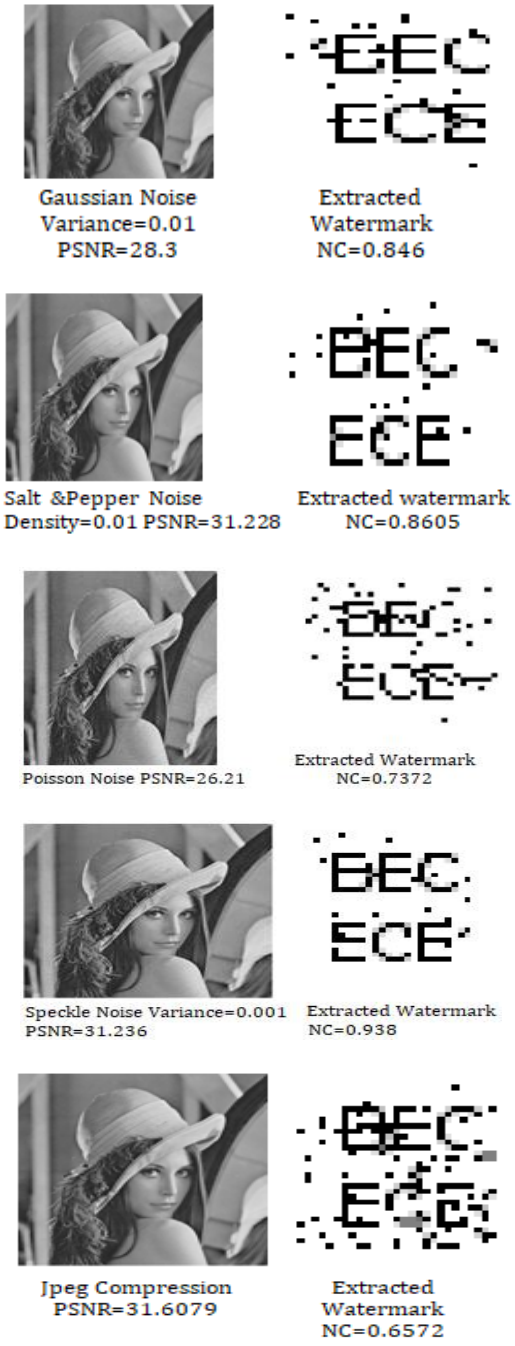
Mean square error

The mean squared error is frequently used to assess the risk of an estimator, it indicates the estimator error that is, how large or on average the losses generated by the estimation errors Zero mean square error indicates that image transmission is lossless. In table 1 Mean Square error were calculated by other researchers for color image using various transforms. Here N represents the number of block of image matrix.

Table 1 Mean Square error for various transform

Transform/ Mean Square Error	N=32	N=64	N=128
Discrete Cosine Transform (DCT)	5.079 E-9	5.640 E-9	6.249 E-9
Malakooti Transform (MT)	0	0	5.749 E-17
Hadamard Transform (HT)	0	0	0

Result of Watermarking



CONCLUSION

A blind digital image watermarking scheme, which embeds watermark in the wavelet domain of an image by using the discrete wavelet packet transform (DWPT) and quantization of the selected dominant coefficients, was proposed in this paper. In addition to this, blind detection of the watermark is applied in this method. It saves the time and space for transferring the original image and saving the original image, respectively. The results of experiments show that the proposed method is very robust against JPEG compression and Gaussian noise. The quantization parameter Δ, which has different

value affects the robustness of the watermark, used in the algorithm is user-defined. It needs a large number of experiments to decide a proper value. Moreover, the capacity, which is an important part of digital watermarking, will also be developed in our future work.

Future Scope

Proposed algorithm may not be suitable for video data as video has more size as compared to image and requires more real times for execution; hence there are possibilities for future development. The future direction of this work is to develop suitable algorithm for multimedia data like video and sound. Another major area for extending the work is by providing lossless and secure video and sound transmission in wire and wireless mode.

REFERENCES

[1]. Qing Liu ,Tianshui Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis 2012 IEEE Symposium on Electrical & Electronics Engineering (EEESYM).

[2]. Anamitra Makur, Nikhil Narayan S."Tamper-Proof Image Watermarking using Self Embedding" Electrical & Electronic Nanyang Technological University, Singapore, acm-2012.

[3]. V. Subramanyam, Sabu Emmanuel and Mohan S. Kankanhalli "Robust Watermarking of Compressed and Encrypted JPEG2000 Images" Member, IEEE Transactions On Multimedia, Vol. 14, No. 3, June 2012.

[4]. Xiangbin Feng, Yonghong Chen. Digital Image Watermarking Based on Super- Resolution Image Reconstruction 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012), 978-1-4673-0024-7/10, IEEE-2012.