Encrypting Watermarked Images: A Transparent Approach

Anjali Bhansali, HiralBarot, KinjalMasrani, Shraddha Shah, and Vicky Chheda

***Abstract*—This paper proposes a method for watermarking gray scale images in spatial domain along with transparent encryption technique for copyright and authentication purpose. Both techniques are independent of each other. Data to be embedded in the image replaces the LSB's of the image with the watermark bits. Encryption process is carried out by initial permutation of watermarked image followed by Hill Cipher technique. Results mentioned below confirm that the watermark can be read with complete success from the encrypted images.**

***Index Terms*—Encryption, watermarking, transparent encryption**

I. Introduction

Although digital data has many advantages over analog data, there is always a fear of unrestricted duplication and dissemination of copyrighted data. Due to the possible copyright issues, the integrity of the data must be protected. For copyright protection and authentication of digital data, two independent techniques are used: Watermarking and Encryption.

Watermarking is used for embedding invisible or visible information into images whereas encryption is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it, only authorized users can read. There are applications in which both encryption and watermarking must be done to achieve authentication as well as to maintain the confidentiality of the image data. In such cases, however, if encryption and watermarking processes are not independent of each other, to authenticate images one will have to decrypt the image first and then retrieve the added watermark. In other words just to authenticate the images confidential data must be disclosed at intermediate nodes through which the data transmission takes place. Hence the is need of designing an approach in which both encryption and watermarking can be done simultaneously and independently in such a way that encryption does not affect the watermark embedded in the images. One such approach was developed in [1]. Encrypting watermarked images in transparent way will help in authentication of images without having to decrypt the images. Such approaches should make optimum use of memory, processing time and cost as considered by the authors in [2] and [3]. Also for encryption to serve the purpose, the algorithm should be such that it should be absolutely reversible as dealt in [4] and [5].

Manuscript received December 19, 2012; revised February 25, 2013.

The authors are with K. J. Somaiya College of Engineering, University of Mumbai, Mumbai, India (e-mail: bhansali_anjali@yahoo.com).

II. Transparent Encryption

Aim is to design watermarking and encryption processes such that the watermark can be read from the encrypted image directly, without having the need to decrypt it. Since the watermarked value is computed without decrypting the original data, one can prove authenticity without actually revealing the information.

Digital Watermarking hides the copyright information which is imperceptible and robust against malicious attacks. Techniques like superimposing an image over an original image in the frequency domain by applying Fast Fourier Transform (FFT) and Discrete Cosine Transform (DCT) can also be used. However, the main problem with these algorithms is their implementation with software and hardware techniques. Also Encryption algorithms like Arnold Transfer, Cat Map are not compatible due to their interdependencies with watermarking schemes.

We propose a method for transparent encryption in which we use LSB Modulation for Watermarking as shown in Fig. 1 wherein we are embedding watermark bits in the least significant bits of the pixels of the original image. Next watermarked image is being encrypted using initial Permutation and Hill Cipher Transposition technique.

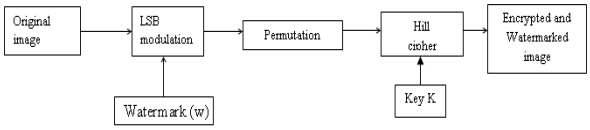

Fig. 1. Watermarking and encryption process

III. Features of the Proposed Method

Our method delivers most of the desirable features as low noise distortions, fair computation speed, imperceptibility etc. Significant features of the method include the following:

- *Imperceptibility* -Only the least significant bit of the selected image pixels is altered to represent the watermark; hence no major visible modification to the content takes place during the process of watermarking.
- *Effective for images of any size* -Works equally well with *small* images and any (m x n) asymmetric sized images.
- Higher computational speed -The watermarking process is not complex and the computational time consumed for generation of watermarked copy is low.
- *Blind* -In blind watermarking methods, extraction of embedded watermark from the watermarked image do not require the original image.

DOI: 10.7763/IJFCC.2013.V2.248

- *Transparency* - In encryption method LSB bits are not used for ciphering, making encryption and watermarking scheme independent of each other.

IV. Watermark Embedding and Encryption Process

The method makes use of the following assumptions.

- If size of original image is (m x n) and that of the watermark is (r x c), then $m > r$ and $n > c$.
- Channel is noise free, or if noisy, there exists suitable error correcting codes to detect and correct all the errors.
- Possible forms of attack include trying to reveal the contents of the original image, or that of the watermark.

A. Least-Significant-Bit Modulation

A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. This technique embeds bits of the message directly into the least-significant-bit plane of the cover image. The advantage of LSB embedding is its simplicity and many techniques use these methods. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. Scaling, rotation, cropping, addition of noise, or lossy compression to the image is very likely to destroy the message.

B. Watermarking Algorithm

As seen from Fig. 1, to watermark the given image, we perform least significant bit (LSB) modulation.

Read the watermark image.

If the watermark bit is 0 or 1, the corresponding location of the original image is made even or odd respectively.

The resultant image obtained is the Watermarked Image.

C. Encryption Procedure

From the Fig. 1 it is clear that the watermarked image is permuted and the transposed using Hill cipher. A key is being used during transposition process which we need not transmit and the resultant image is an encrypted and watermarked image. As mentioned above in (B), watermark is inserted into the LSB of original image. Hence the encryption process proposed is such that it does not alter the LSB. In the proposed algorithm we are using Hill Cipher. Since Hill Cipher is more prone to attacks, we first permute all the bits excluding LSB using a predetermined permutation block.

1) Permutation

Primarily, the LSB is stored in a separate matrix (lsbmat). Each pixel value of the original image is passed through a permutation block. This block permutes the bits of each pixel as per the predetermined order. Then the seven bits are divided into two blocks of four bits (p1) and three bits (p2) respectively. Each block is left shifted by one bit (p3, p4) and concatenated to form a single block (b).

2) Hill cipher transposition

Permuted image matrix (b) is parsed into block of 4×4 (d). Each block is successively transposed by transposition matrix (Key, k) into cipher block (h), where h is given as h= (d×k) mod 256 as by author in [1]. LSB is appended into the resultant matrix (h) to give final encrypted image matrix (a_w_e).

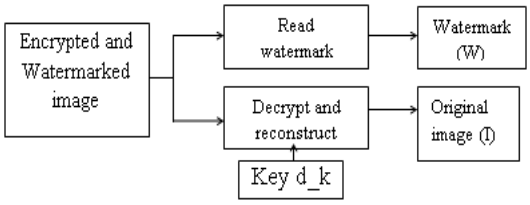

Fig. 2.Transparent decryption process

V. Watermark Retrieval and Decryption Process

Fig. 2 describes the transparency of our algorithm. The encrypted and watermarked image can be decrypted to retrieve the original figure without watermark being affected or we can retrieve the watermark without decrypting the original image.

A. Watermark Retrieval

Retrieving the watermark from the processed image (a_w_e).This is done as follows:

From a_w_e image as per the logic if the decimal equivalent is even or odd then the watermark bit is 0 or 1 respectively.

The extracted watermark bits obtained are assembled and then matched with the original watermark.

B. Decryption process

The LSB of the encrypted and watermarked image (a_w_e) is removed and stored into a matrix (d_lsbmat). The matrix (d_new) thus obtained is parsed into block of 4×4 (d_d). Each block is successively multiplied by inverse of transposition matrix (Key, d_k), which is obtained by performing reciprocal modulo on Key k, into a matrix (d_h), where d_h is given as d_h= (d_d×d_k) mod 256. The resultant matrix (d_b) consist all the permuted values.

Seven bits of each pixel value is divided into two blocks of four bits (d_p3) and three bits (d_p4) respectively. Each block is right shifted by one bit (d_p1, d_p2) and concatenated to form a single block (d_p). This block is passed through a permutation block which permutes the bits as per a predetermined order. Now the LSB (d_lsbmat) is appended into the matrix to give final decrypted image (d_I).

Fig. 3. (From top clockwise) (a) Original image, (b) Watermark, (c) Watermarked image, (d) Retrieved watermark, (e) Decrypted image, (f) encrypted image

VI. Simulation Results

The method proposed in this paper when implemented produced the results shown in Fig. 3. The original image is shown in Fig. 3 (a) along with watermark image in (b). Fig. 3 (c) and (d) show watermarked and encrypted images respectively. Image in Fig. 3 (e) is decrypted image. And image in (f) is the retrieved watermark from the encrypted image of Fig. 3 (d) illustrating the transparency of the encryption process to watermarking. The Peak Signal to Noise Ratio of the original image and retrieved image is formulated as in Table I.

TABLE I: The Peak Signal to Noise Ratio of the Original Image

Image	PSNR
Original	48.0624
Retrieved	48.1308

VII. Conclusion and Future Work

In this paper we have proposed algorithm to authenticate an encrypted image by retrieving the watermark without decrypting the image. Thus making the authentication process independent (transparent) of encryption. In other words, authentication and encryption process are two independent entities. This can be applied on biometric images where authentication is required provided that the secrecy is maintained.

As a future work one may plan to use stronger watermarking algorithms LSB modulation is not flexible and limited to binary images. Study of attacks can be carried out as Hill Cipher is prone to plaintext attacks and if there is any error in the Transposition matrix (Key k) or inverse Key, d_k, then the cipher matrix obtained will deviate from the expected values. This will be almost impossible to decrypt due to error being propagated.

References

[1] A. Talwai, D. Sengupta, and K. Karthik, "A transparent encryption scheme for watermarked biometric and medical images," *International Journal of Computer and Electrical Engineering*, vol. 4, no. 3, June 2012.

[2] D. Anand and U. Niranjan, "Watermarking medical images with patient information," in *Proc. of IEEE/EMBS Conference*, pp. 703-7-6, 1998.

[3] U. R. DeepthiAnand, P. SubbannaBhat, and U. C. Niranjan, "Compact storage of medical images with patient information," *IEEE Transactions on Information Technology in Biomedicine*, vol. 5, no. 4, December 2001.

[4] B. Acharya, G. Rath, S. SPatra, and S. K. KPanigrahy, "Novel methods of generating self-invertible matrix for hill cipher algorithm," *International Journal of Security*, vol. 1, no. 1, pp. 14-21, 2007.

[5] R. A. Hamamreh and M. Farajallah, "Design of a robust cryptosystem algorithm for non-invertible matrices based on hill cipher," *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 5, May 2009.

Anjali Bhansali is an under graduate student at K. J. Somaiya College of Engineering, University of Mumbai, Mumbai, India.

Hiral Barot is an under graduate student at K. J. Somaiya College of Engineering, University of Mumbai, Mumbai, India.

Kinjal Masrani is an under graduate student at K. J. Somaiya College of Engineering, University of Mumbai, Mumbai, India.

Shraddha Shah is an under graduate student at K. J. Somaiya College of Engineering, University of Mumbai, Mumbai, India.

Vicky Chheda is an assistant professor at K. J. Somaiya College of Engineering, University of Mumbai, Mumbai, India. He holds M.Tech degree in Digital Signal Processing (DSP) from the Indian Institute of Technology (IIT) Guwahati and BE degree in mmunications from University of Mumbai.