# A Selective Bitplane Based Encryption of Grayscale Images with Tamper Detection, Localization and Recovery Based on Watermark

**Sukalyan Som, Sayani Sen, Suman Mahapatra and Sarbani Palit**

**Abstract** Ciphered data need an additional level of protection in order to safeguard them from being tampered after the decryption phase. Ciphered data, upon being deciphered by the intended receiver, is unprotected and it can be easily doctored by ever-developing, sophisticated image processing softwares. In the proposed scheme, we introduce a selective bitplane based encryption of grayscale images coupled with the facility of tamper detection, localization and restoration based on DWT based digital watermark. The original image is first sub-divided into blocks where Discrete Wavelet Transform (DWT) is applied to generate the watermark. This is embedded in four disjoint portions of the image to increase the probability of restoration of the tampered image from tampers. To add another level of security to the transmission of the watermarked image a selective bitplane based encryption based on chaos is applied. The watermarked image is first partitioned into its constituent bitplanes and then first four bitplanes from Most Significant Bitplane (MSB) is encrypted by a chaos based pseudorandom binary number generator (PRBG). The enciphered bitplanes are concatenated with unencrypted ones to produce the cipher watermarked image. The validity and novelty of the proposed scheme is verified through exhaustive simulations using different images of two well-known image databases.

S. Som (✉)
Department of Computer Science, Barrackpore Rastraguru Surendranath College, Barrackpore, Kolkata, India
e-mail: sukalyan.s@gmail.com

S. Sen · S. Mahapatra
Department of Computer Science and Engineering, University of Kalyani, Kalyani, India
e-mail: sumancse19@gmail.com

S. Mahapatra
e-mail: sayani.sen@gmail.com

S. Palit
CVPR Unit, Indian Statistical Institute, Kolkata, India
e-mail: sarbanip@isical.ac.in



J.K. Mandal et al. (eds.), *Information Systems Design and Intelligent Applications*, Advances in Intelligent Systems and Computing 339,
DOI 10.1007/978-81-322-2250-7_79

**Keywords** Discrete wavelet transform · Chaos · Cryptography · 1D logistic map · Information entropy · Peak-signal-to-noise-ratio (PSNR)

## 1 Introduction

Visual information in the form of images and videos has become an inevitable part of modern civilization with the advent of sophistications in transmission of them through internet. Transmitted images may have different applications viz. commercial, military and medical applications. So it is necessary to encrypt image data before transmission over the network to preserve its security and prevent unauthorized access. In recent years number of different image encryption schemes has been proposed in order to overcome image encryption problems. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption [1–5]. Since the last decade a different approach for content protection has gained attention of researchers. To overcome the computational complexity, reduce the cost of encrypting digital images and to facilitate real time transmission with lesser bandwidth requirement the idea of encrypting only portion of data, termed as partial encryption in many occasions, is preferred. Selective bitplane based encryption of digital images may refer to partial encryption where only some bitplanes are encrypted depending their relevance and significance. In [6] an analysis of the security of the selective bitplanes based encryption is performed. It has been demonstrated that, when more than the MSB is selected for the ciphering procedure, the reconstructed image, obtained by replacement attack, is severely affected. While cryptographic measures are employed to protect the privacy of the information during transmission, watermarking techniques are suitable for copyright protection. Tampering of digital media and its detection has been an interesting problem since long. Digital watermarks are used not only to protect authentication of digital data but also to provide means to localize the tamper made and attempt to restore as close as possible to the original one. Recent research has started focusing on the possibility of providing both the security services simultaneously as encrypted data becomes vulnerable for being tampered by the fraudulent receiver after decrypting it. Despite the difficulties of realizing effective algorithm that combine simultaneously watermarking and selective bitplane based encryption, some solutions have been proposed [7–10].

In this communication, an attempt is made to propose a selective bitplane based encryption of grayscale images coupled with the facility of tamper detection, tamper localization and restoration by DWT based digital watermark. The original image is first sub-divided into non-overlapping blocks of size $2 \times 2$ where 1 level 2D DWT is applied to generate the watermark which is then embedded in four disjoint portions of the image to increase the probability of restoration of the tampered image. To add another level of security to the transmission of the

watermarked image a symmetric key selective bitplane driven encryption based on chaos is applied. The watermarked image is first partitioned into its constituent binary bitplanes and then first four bitplanes from Most Significant Bitplane (MSB) is encrypted by a chaotic PRBG formed by the use of 1D Logistic maps. The enciphered bitplanes are concatenated with unencrypted ones to produce the cipher watermarked image.

The rest of the paper is organized as follows: In Sect. 2, the proposed scheme is explained with experimental results and their analysis being done in Sect. 3. Section 3 presents the comparison of the scheme with existing State-of-art. Finally, conclusions are drawn in Sect. 4 where future directions of work is also mentioned.

## 2 Proposed Scheme

An encrypted image becomes vulnerable for being tampered after being decrypted at the receiver end. Thus to preserve the authenticity of an image being transmitted in encrypted form is preserved by embedding a watermark, generated from the image itself, before encryption. The watermark is used for tamper detection, localization and restoration up to a great extent. Thus the proposed scheme consists of two parts—watermark embedding and encryption (sender), decryption and watermark extraction: tamper detection, localization and restoration (receiver).

### *2.1 Watermark Generation and Embedding*

- An image $I_{org}$ of size $2^n \times 2^n$, $n \in N$ and $n \geq 2$ is sub-divided into non-overlapping $2 \times 2$ sized blocks.
- A look-up table constructed using Eq. (1) that holds the mapping address of each block in $I_{org}$.

$$X' = [f(x) = (k \times X) \; mod \; N] + 1 \tag{1}$$

  where $X, X'(\in [0, N-1])$ the block number, $k(a\ prime\ and\ \in Z - \{factors\ of\ N\})$ a secret key and $N(\in Z - \{0\})$ the total number of blocks in the image.
- A push-aside operation modifies the lookup table by pushing right the columns belonging to the left half and viceversa.
- 2-D DWT is applied on each block using the Haar wavelet. The approximation coefficient matrix $LL_1$ and detail matrices $HL_1$, $LH_1$ and $HH_1$ are produced. The watermark is generated from $LL_1$ sub-band coefficient.
- $I_{org}$ is divided horizontally and vertically into four disjoint and equal parts. A block (say, $A$) and its partner block (say, $C$) can be located at the same positions of two parts situated at opposite angles.

- The 12-bit watermark for block $A$ and its partner block $C$ is constructed by combining five MSBs of $LL_1$ sub-band coefficient of the block $A$, five MSBs of $LL_1$ sub-band coefficient of its partner block $C$, in–block parity–check bit $p$ and its complementary bit $\upsilon$.
- The 12-bit watermark generated from a block ($A$) and its partner block ($C$) is embedded into their mapping blocks ($\bar{A}$ and $\bar{C}$). The 3 LSBs of each of the 4 pixels of a mapping block are replaced by the 12-bit watermark.

## 2.2 Image Encryption

- Each pixel of watermarked image $I_{org}^{W}$ is decomposed into its corresponding 8 bit binary equivalent and thus 8 bit-planes $BP_i(x, y) \forall i = 1, 2, \ldots, 8$ are formed.
- Keys for diffusing the significant bitplanes are generated using 1D Logistic map based PRNG with chosen values of the triplet $(x_0, y_0, \mu)$. The PRBG is based on two 1D Logitic maps stated in Eq. (2)

$$x_{n+1} = \mu x_n(1 - x_n) \; and \; y_{n+1} = \mu y_n(1 - y_n) \tag{2}$$

where $x \in [0, 1]$ and $\mu \in (3.57, 4]$. The bit sequence is generated by comparing the outputs of both the maps as in Eq. (3)

$$\begin{aligned} g(x_{n+1}, y_{n+1}) &= 1; \; if \; x_{n+1} \geq y_{n+1} \\ &= 0; \; if \; x_{n+1} < y_{n+1} \end{aligned} \tag{3}$$

- The first four bitplanes considered as the significant ones, are encrypted as $CBP_j = BP_j \oplus K_j \; \forall j = 1, \ldots, 4$. The cipher bit planes $CBP_j$ and the unencrypted bitplanes $BP_i$ are combined together to form the cipher image as $C_i(x, y) = CBP_j + BP_k \; \forall i = 1, 2, \ldots, 8, \; j = 1, \ldots, 4$ and $k = 5, \ldots, 8$ where $+$ is used to denote concatenation.

## 2.3 Image Decryption

Upon receiving the encrypted image along with the key $(x_0, y_0, \mu)$ one will perform decryption in a manner reverse to that outlined in Sect. 2.2 to get the decrypted image.

## 2.4 Watermark Extraction: Tamper Localization and Restoration

The embedded watermark has to be extracted in order to detect and localize tamper and restore from it. Three types of tamper has been considered in this literature—Direct Cropping, Object Insertion and Object manipulation. The procedure is stated below. A 3-level hierarchical tamper detection and localization is performed, the algorithm for which is described below.

**Tamper detection and localization** In level 1, for each block B

- Retrieve the 12-bit watermark from B.
- Get the parity-check bits p and v respectively from the 11th and 12th bits of the watermark.
- Perform XOR operation on the 10 LSBs of the 12-bit watermark, resulting in $p'$.
- If $p = p'$ and $p \neq \upsilon$, mark block B valid, else invalid.

In Level 2, for each block B marked valid after Level 1 detection

- If at least one of the four triples (N, NE, E), (E, SE, S), (S, SW, W), (W, NW, N) of the $3 \times 3$ neighborhood of block B has all of its blocks marked invalid, mark block B invalid.

In Level 3, for each block B marked valid after level 2 detection

- If at least five of the $3 \times 3$ neighboring blocks of block B are marked invalid, mark block B invalid.

**Restoration of image from tamper** A two-stage restoration scheme is applied for recovering the invalid blocks.

In Stage 1: For each nonoverlapping block B of size $2 \times 2$ pixels marked invalid

- Find the mapping block $B'$ of $B$ from the look-up table.
- If $B'$ is valid then $B'$ is the candidate block, go to the last step here.
- Find the mapping block of $B'$'s partner-block $B''$.
- If $B''$ is valid then $B''$ is the candidate block; otherwise stop, leave block B alone.
- Retrieve the 12-bit watermark from the candidate block.
- If block B is located in the upper left or lower right quarter of the image, the 5-bit representative information of block B starts from the 1st bit (MSB) of the 12-bit watermark; otherwise, it starts from the 6th bit.
- Pad four 0s (as LSBs) to the 5-bit representative information to form a new 9-bit coefficient.
- Perform the inverse DWT operation based on this coefficient as the approximation coefficient resulting in a new block of size $2 \times 2$.
- Replace block B with this new block and mark block B as valid.

In stage 2 After stage 1 recovery

- Recover the remaining invalid blocks from the pixels of the neighboring blocks represented as directional triples (N, NE, E), (E, SE, S), (S, SW, W) and (W, NW, N) surrounding them.
- Finally, the lost blocks are generated by interpolating pixel values.

## 3 Experimental Results, Tests and Analysis

The proposed algorithm has been exhaustively simulated and its performance has been tested over commonly used and widely accepted USC-SIPI [11] image database, maintained by Signal and Image Processing Institute, University of Southern California. The *misc* volume of the database has been chosen in this literature to prove the efficacy of the proposed scheme. The proposed scheme and the existing state-of-the-art, considered for comparison, have been implemented using Matlab 7.10.0.4 (R2010a) on a system running with Windows 7 (32 bit) with Intel Core i5 CPU and 4 GB DDR3 RAM. In Fig. 1 a thumbnail view of the images considered from the *misc* volume of the database is shown. In Fig. 2 an original image of Lena, its watermarked image, the ciphered watermarked image, and the decrypted image are shown. To prove the efficacy of the proposed algorithm tests has been performed on the encrypted image and the decrypted image (watermarked) separately.

### *3.1 Tests on Encryption*

**Histogram Analysis** In order to have a perfect ciphered image the histogram of the image must exhibit uniformity of distribution of pixels against the intensity values.

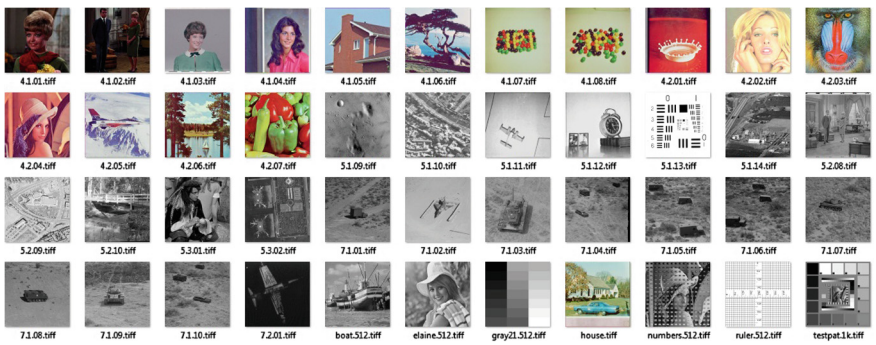


**Fig. 1** A thumbnail view of the *misc* volume of USC-SIPI image database

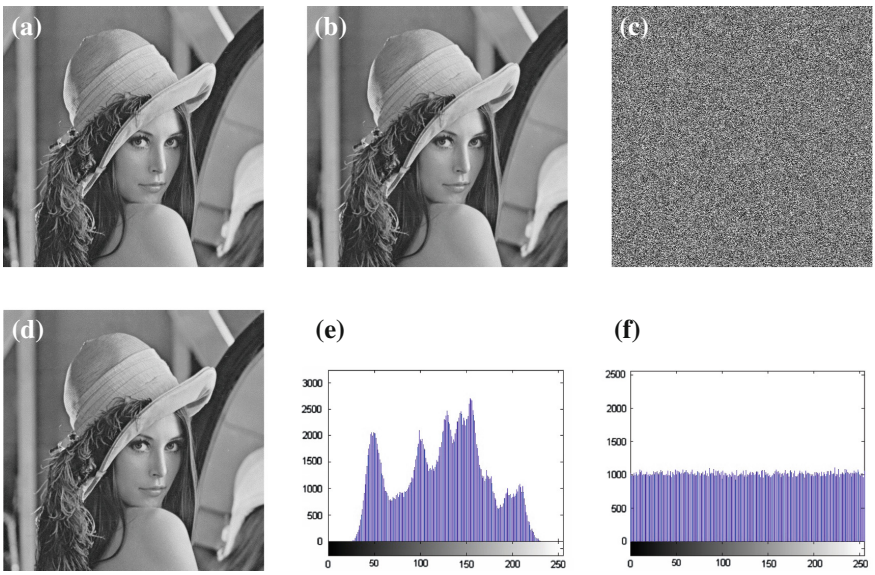


**Fig. 2** **a** Original image, **b** watermarked image, **c** encrypted watermarked image, **d** decrypted image, **e** Histogram of (**b**), **f** histogram of (**c**)

The histograms of original and encrypted images have been analysed. In Fig. 2e, f the histograms of the watermarked image of Lena of size $512 \times 512$ and corresponding cipher image has been presented which depicts that the histograms of plain image has certain pattern where as that of the cipher image are uniformly distributed.

**Correlation Coefficient Analysis** It is observed that there exists high correlation among adjacent pixels in an original image but poor correlation between the neighbouring pixels of corresponding cipher image. Karl Pearson's Product Moment correlation coefficient is used to find the correlation of horizontally, vertically and diagonally adjacent pixels of both the plain and cipher image and the correlation between the plain image and cipher image pixels. The average values of correlation coefficient of the horizontally adjacent pixels in watermarked and cipher image are 0.9804 and 0.0018 where as that the same in vertically adjacent pixels are 0.9725 and 0.0008 respectively. The correlation coefficient between the watermarked image and their ciphered image is 0.0008.

**Key sensitivity and key space analysis** A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secret keys in encryption process results into a completely different encrypted image and in the decryption process original image is not found. A good encryption scheme must have a large key space to make brute force attack infeasible. In the proposed algorithm, the initial conditions and the system parameters of the chaotic maps i.e. the triplet $(x_0, y_0, \mu)$ forms the symmetric key. Considering the precision of

calculation as $10^{-14}$ the key space for the proposed scheme is $10^{14} \times 10^{14} \times 10^{14} = 10^{42}$ which is reasonably large enough to resist the exhaustive attack.

**Information Entropy Test** It is well known that the entropy H(s) of a message source s can be calculated as:

$$H(s) = \sum_{i=1}^{2^N-1} p(S_i) \cdot \log_2 \frac{1}{p(S_i)} \tag{4}$$

where $p(S_i)$ is the probability of symbol $S_i$ and the entropy is expressed in bits. When the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. In our algorithm the average of entropy of the cipher images is 7.9997 which is close to ideal value.

## 3.2 Use of Watermark: Tamper Detection, Localization and Recovery

**Measurement of watermark and encryption Quality** To measure the imperceptibility of watermark and encryption quality well known metrics viz. PSNR and SSIM is used. For an encrypted image smaller PSNR and SSIM is expected where as for the watermarked image to be imperceptible a PSNR greater than 35 dB and SSIM close to unity exhibits better image quality. The average PSNR and SSIM of the watermarked image is 41.5 and 0.97 dB respectively where as the PSNR for encrypted version of the watermarked image is dB.

**Performance against tampering** To evaluate the effectiveness of the proposed scheme against tampering, localize the tampers, and restore them back as close as possible to the original, the decrypted watermarked images went through different types of tampers—Direct Cropping, Object Insertion and Object manipulation. An watermarked image cropped at different positions ranging from as small as 5 % to as large as 95 % with the PSNR of restored image from 42.05 to 19.87 dB. The average PSNR of restored image is 31.5 dB. One of the most common image tampering attack is insertion of objects is by copying regions of the watermarked image and pasting them into somewhere else in that image. The proposed watermarking system detects, localizes, and recovers the tampered regions of the images tampered by inserting small, medium, and large objects. The proposed scheme is capable of restoring an attacked image by removing, destroying, or changing specific regions or objects in it. In Fig. 3 the results of tamper detection, localization and restoration is presented.

**Fig. 3** The results of different tampers and their restored versions

## 4 Conclusion and Future Scope

Our results show that encrypting only a part of the image is sufficient to conceal significant information while reducing the complexity of encrypting the entire image. Embedding a DWT based watermark, generated from the image itself provides a solution to detect and localize tampers done in the decrypted image while providing the option to restore it as close as possible to the original one. Further research will be carried out to improve the performance for situations where very small areas are tampered.

## References

1. Lian, S., Sun, J., Wang, Z.: A block cipher based on a suitable use of chaotic standard map. Chaos Solitons Fractals **26**(1), 117–129 (2005)
2. Pisarchik, A.N., Flores-Carmona, N.J., Carpio-Valadez, M.: Encryption and decryption of images with chaotic map lattices. CHAOS J. **16**(3), 033118-033118-6. American Institute of Physics (2006)
3. Pareek, N.K., Patidar, V., Sud, K.K.: Image encryption using chaotic logistic map. Image Vis. Comput. **24**(9), 926–934 (2006)
4. Dongming, C., Zhiliang, Z., Guangming, Y.: An improved image encryption algorithm based on chaos. In: Proceedings of IEEE International Conference for Young Computer Scientists, pp. 2792–2796 (2008)
5. Som, S., Kotal, A.: Confusion and diffusion of grayscale images using multiple chaotic maps. In: National Conference on Computing and Communication Systems (NCCCS) (2012)
6. Podesser, M., Schmidt, H.-P., Uhl, A.: Selective bitplane encryption for secure transmission of image data in mobile environments. In: 5th Nordic Signal Processing Symposium in Mobile Environments
7. Lian, S., Liu, Z., Wang, H.: Commutative watermarking and encryption of media data. Optical Eng. Lett. **45**(8), 080510 (2006)
8. Lian, S., Liu, Z., Ren, Z., Wang, H.: Commutative encryption and watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol. **17**(6), 774–778 (2007)

9. Schmitz, R., Li, S., Grecos, C., Zhang, X.: A new approach to commutative watermarking-encryption. In: CMS 2012, LNCS 7394, pp. 117–130 (2012)
10. Schmitz, R., Li, S., Grecos, C., Zhang, X.: Towards more robust commutative watermarking-encryption of images, In: IEEE International Symposium on Multimedia, pp. 283–286 (2013)
11. USC-SIPI image database available at http://sipi.usc.edu/database. Accessed 27 Feb 2014