Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching

Sanjeev Narayan Bal, Manas Ranjan Nayak, Subir Kumar Sarkar

Department of ETCE, Jadavpur University, Kolkata 32, India

ARTICLE INFO

Article history:
Received 12 December 2017
Revised 10 April 2018
Accepted 13 April 2018
Available online xxxx

Keywords:
Watermarking
Cryptography
Least significant bit
Bit pairs similarity
Matching

ABSTRACT

Watermarking is one of the most vital digital information hiding technique, which can be used with cryptography mechanism for providing more security to digital data. In image watermarking mechanism mostly LSB substitution is used on the cover image for hiding the secret watermark. In this paper, a novel technique based on the matching of bit pairs and symmetric key cryptography is proposed. Pixel bits of original image and encrypted watermark image are arranged in pairs. The pixel bits are represented in pairs following the proposed algorithm, then the encrypted watermark pixel bit pairs are compared with all bit pairs of original image and accordingly the replacement of bit pairs takes place with the respective matched pair assigned number binary equivalent. If no match is found then go for replacing the 0th pair with watermark bits and replace the two LSB with the value of pair number 0. The proposed mechanism shows good quality of watermarked image along with good PSNR values with a good payload. By comparing the results with some existing algorithms, the proposed scheme shows the valuable results.

1. Introduction

For copyright protection of multimedia information, a variety of digital watermarking techniques have been developed, which are used to protect the multimedia information from being abused. There are two categories of techniques of embedding the watermark for copyright shield in any multimedia information, be it the image, audio or video. The spatial domain technique follows any particular algorithm for embedding of the watermark by directly adding it to the data, and the frequency domain method is to embed it in any of the transform domain. The spatial domain of watermarking is faster but fails in robustness while the frequency domain watermarking is robust but still consumes more resources in terms of power consumption and slower speed of computing (Acken, 1998; Low et al., 1998; Macq and Pitas, 1998; Swanson et al., 1998).

It is better to go for the higher cost of computing to get the benefits of robustness of the watermark when maliciously attacked by the mechanisms of noise, filtering or compression. For the realization of the watermarking mechanisms, the major areas of focus are imperceptibility, robustness, capacity, security, and trustworthiness. The perceptual transparency of the hidden data or information is the imperceptibility. Survival of the watermark information against intentional or unintentional attacks without significant degradation of the quality of the original image is the robustness. The payload for the new signal is defined as the capacity and the undetectability of the watermark information on the corresponding media, which is defined as the security and all these turned to be very important considerations in case of invisible watermarking (Liu and Tan, 2002; Zhu et al., 2006; Gutab and Ghouti, 2007). A well-known survey of watermarking techniques can be found from (Kutter and Hartung, 1999; Mohanty, 1999; Altaibi et al., 2015). There is a trade-off between these parameters as an increase in robustness may appear at the expense of enhanced watermark signals visibility as well as reduced bandwidth. But, the perceptual distortion of the image, due to watermark embedding is not related directly to the magnitude of the watermark signal. It can be observed that the watermark signal of same strength is causing less visual distortion in busy areas of the image than the flat background. In the papers (Podilchuk and Wenjua, 1998; Hannigan et al., 2001) on watermarking, there is less effort to evaluate images in order to consider the upper limit of the power of the watermark signal without considerable visual distortion. These spatial domain methods neglect the significance

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

E-mail address: s_n_bal@yahoo.co.in (S.N. Bal)

https://doi.org/10.1016/j.jksuci.2018.04.006
1319-1578/© 2018 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

of payload capacity and mostly focused on the imperceptibility factors. In Khan and Gutub (2007) the authors proposed an image based message concealment mechanism by use of punctuation marks to encode a secret message and by using modified scytale cipher provides the better result as far as the security is concerned. In Al-Otaibi (2014) the author proposed a data hiding technique with two layers of the security system by including AES cryptography followed by image-based steganography to ensure high security. Methods of LSB matching is proposed in Sharp (2001), which also called ± embedding mechanism (Li et al., 2011). In this method, the cover image pixel value is increased or decreased randomly by one when the secret bit is not equal to the LSB of the pixel belonging to the cover image (Huang et al., 2014). The LSB-M modifies both the histogram of an image and the correlation between the adjacent pixels, which helps the steganalysis methods to attack this method (Xia et al., 2016). In Sabeti et al. (2013) the authors proposed complexity based LSB matching scheme, where the LSB matching is used in order to enhance the security against possible attacks. This mechanism uses a local neighborhood analysis to determine the secure locations of an image and then LSB matching used for the embedding process. In Parvez and Gutub (2011) the authors proposed one image steganography algorithm, which determines the number of secret message bits that each pixel of the cover image can store based on a partition scheme of color intensity range. This scheme provides high data hiding capacity and security for the host image.

2. Related works

In this segment, we offer a brief review related to LSB matching and other mechanisms of LSB. The work in Wu and Tsai (2003) proposed pixel value differencing mechanism in which a pixel value differencing is used to differentiate between edge areas in comparison to smooth areas. Consequently, the payload of the embedded data is higher in edge areas than that of areas of smooth. Recently the authors proposed certain mechanisms combining PVD and LSB replacement for better embedding efficiency (Chang and Tseng, 2004). A number of methods were proposed by combining PVD and LSB replacement mechanisms (Mahjabin et al., 2012; Khodaei and Faez, 2012; Mandal and Das, 2012). In Gutub et al. (2009) the authors proposed a good algorithm on steganography by merging the idea of random pixel manipulation methods and the stego key ones. This mechanism shows good outcomes of hiding capacity with relation to the RGB image pixels. In the paper (Sumathi et al., 2014) a mechanism developed called LSB-MR(Least Significant Bit Matching Revisited). In this method, the embedding process is carried on a cover pixel pair at a time to embed the secret bit pair. The corresponding stego pixel pair can be formed by keeping that cover pixel pair unaltered or by increasing or decreasing the value by one. A function is used here to evaluate the need for alteration to cover pixel values. Practically this mechanism reflected poor embedding rate. To generalize this mechanism a LSB-M(Matching) method was proposed in Li et al. (2009). To enhance the security of both LSB-M and GLSBM, a content adaptive mechanism proposed by the authors (Wang et al., 2010). In Sabeti et al. (2013) the authors proposed a LSB-M adaptive algorithm called complexity based LSB-M in which a complexity region is determined for embedding of data by using an 8-neighborhood of a pixel. The disadvantage of this mechanism was low embedding capacity. In the paper (Tsai et al., 2016) the mechanism based on interpolation, LSB substitution, and histogram shifting. The interpolation process is used to adjust embedding capacity for low distortion of the image, the embedding is then applied using LSB substitution and shifting of histogram mechanism.

In Akhtar (2015) the authors suggested an improved LSB substitution mechanism. In this process, secret data is hidden after compressing the smooth areas of the image losslessly resulting in lesser number of modified cover image pixels. Then a bit inversion mechanism is applied where certain LSBs of pixels are modified if they occur in a specific format. In Jung and Yoo (2015) the authors suggested a mechanism of semi reversible data hiding based on interpolation and LSB substitution. Initially, interpolation is used to scale up and down the cover image before hiding the secret watermark to achieve high embedding capacity with very low distortion of the image quality. In Al-Otaibi and Gutub (2014) the authors proposed an image based steganography replacing the pixel, least significant bit with hidden text. The scheme experimentally explores the data dependency and its security issues with attractive results. In Abu-marie et al. (2010) the authors proposed a LSB replacement based technique using truth table based and determinate array on RGB indicator that uses pixel manipulation, shows amazing results in data hiding capacity. In Gutub et al. (2009) the authors suggested an image based steganography technique called triple-A, using LSB bits of image pixels with more randomization in the selection of a number of bits and using color channels. This mechanism adds more security to data hiding process. In Yang et al. (2008) the authors proposed the edge based LSB mechanism with high embedding capacity, but the security issue was very poor. In the paper (Hempstalk, 2006) the authors suggested a mechanism to hide the information bits in the less focused areas such as corners of the original cover image. But, the disadvantage of this mechanism is that the payload capacity is very low. In Luo et al. (2010) the author proposed a mechanism which uses a pseudo-random number generator with LSB matching to select the location for data hiding into the original cover image. This mechanism exploits sharper regions into the host image to hide more data bits as compared to smoother areas. In the paper (Wang et al., 2008) the authors used the PVD and LSB mechanisms to hide fewer data bits in the cover images. This mechanism uses the difference in the pixels and a modulus function to secure data bits by changing the remainder or value of modulus.

In this paper, we proposed a cryptography-based bit pairs matching watermarking mechanism in the spatial domain and used the symmetric key cryptography (Menezes et al., 1996; Roy et al., 2011) to encrypt the watermark to protect the information from the intruder during transmission. The objective of the proposed mechanism is to improve the robustness of enhanced payload and security while maintaining the imperceptibility.

3. Watermark embedding and extraction

In this segment, the process of watermarking is explained. The aim of this work is to increase the watermark strength by embedding the watermark following a new mechanism of cryptography and bit pairs matching.

3.1. Symmetric key cryptography

The security of the projected mechanism is enhanced by adding encryption. The watermark is encrypted by using symmetric key cryptography, which protects the contents of multimedia information from attackers. This encryption mechanism uses a single key to encrypt the grayscale watermark logo in encoding section as well as decrypt the watermark logo in decoding section. During the encryption process, the algorithm 1 is used here to convert each pixel of the watermark logo into binary, reverse it and store the quotient and remainder by dividing the reversed string by a key. The process of decryption used the algorithm 2, in which the same key is used to receive the original image pixels (Roy et al., 2011)

```
Algorithm 1: Watermark Encryption
Input: Grayscale image
1: Consider the grayscale image W.
2: Generate the decimal value for each pixel ($P_i$) of W.
3: Find out the corresponding binary value ($B_v$) of each $P_i$.
4: Reverse that 8 digit's binary number $B_v$ to get $R_v$.
5: Consider a 4 digit divisor as the Key ($K_e$).
6: Now divide the reversed number $R_v$ with the divisor $K_e$.
7: Next store the remainder and quotient in an 8-bit string. If
   required, add the number of 0s on the left-hand side of
   remainder and quotient bits to complete the 8-bit string.
   This leads to being the encrypted data (ED).
Output: Encrypted image
```

```
Algorithm 2: Watermark Decryption
Input: Encrypted image data (ED) and the key ($K_e$)
1: Multiply the quotient bits of the encrypted data (ED) by the
   Key ($K_e$) to produce F.
2: Add the remainder bits of the encrypted data (ED) with the
   result produced in the above step (F) to get G.
3: If the result produced (G) in the previous step i.e. step 2 is
   not an 8-bit number, then we require, making it an 8-bit
   number.
4: Reverse the number G to get the decrypted data (DD).
Output: Decrypted image
```

3.2. Encoder

Let A be the original grayscale cover image with size pXq and represented as

$$A = X(i,j); 0 \leqslant i < p, 0 \leqslant j < q, X(i,j) \in \{0, ----------, 255\}. \quad (1)$$

Let B be the original grayscale watermark logo with the size of rXs and can be represented as

$$B = Y(i,j); 0 \leqslant i < r, 0 \leqslant j < s, Y(i,j) \in \{0, ----------, 255\}. \quad (2)$$

After applying the encryption process as per algorithm 1, the watermark logo changed to Wc and can be defined as

$$Wc = Y_c(i,j); 0 \leqslant i < r, 0 \leqslant j < s, Y(i,j) \in \{0, ----------, 255\}. \quad (3)$$

Now consider the Wc and consider individual pixels of it. Convert each pixel to its binary equivalent, and then make the pairing of the binary bits (Fig. 1).

Now consider each pixel of the original image A and convert it to its binary equivalent and form four pairs out of that by choosing 4th and 3rd bits as the 0th pair, 5th and 4th bits as 1st pair, 6th and 5th bits as the 2nd pair, 6th and 7th bits as the 3rd pair. Now consider the matching of pair bits of encrypted watermark W_c with individual pixels bit pairs of A. If the 1st pair of bits of W_c and 3rd pair of bits of A are matched then replace two LSB of the respective pixel of A with the 3rd pair number as (1,1). If the pair do not match then the mechanism compares the respective bit pair of the pixels of W_c with the 2nd pair of the respective pixels of A. If matching is there, then replace two LSB of the respective pixel with the 2nd pair number (1,0) of A. Still if there is no match then go for a matching with 1st pair of data bits of respective pixels of A. If matched then two LSB will be replaced with the number assigned

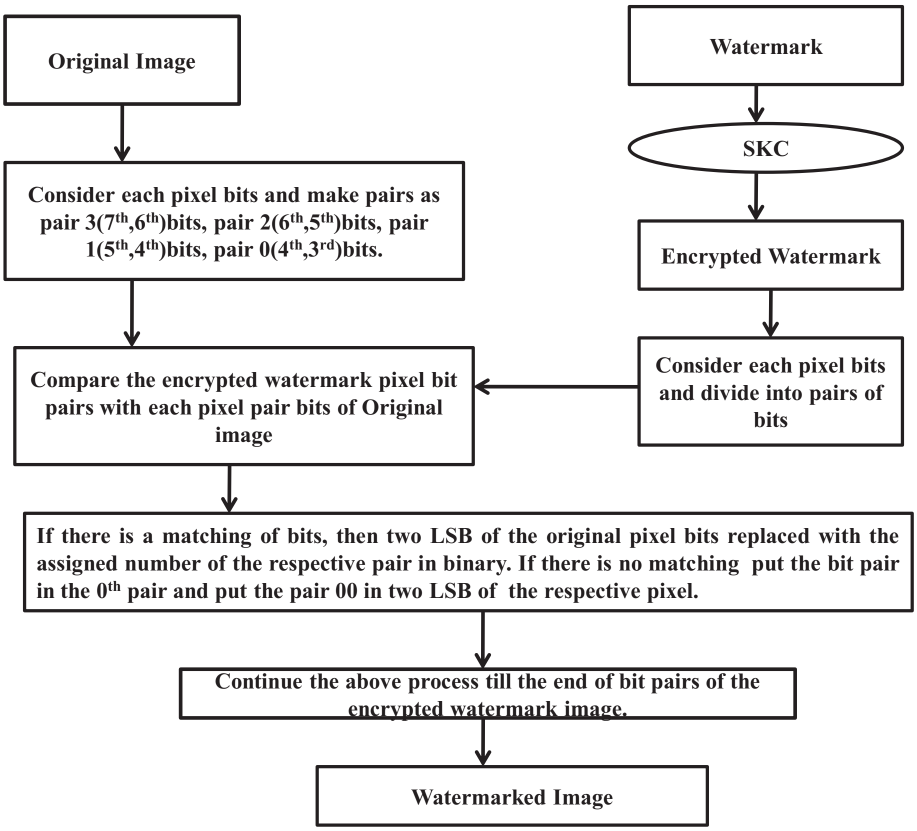

Original Image
Consider each pixel bits and make pairs as pair 3(7th,6th)bits, pair 2(6th,5th)bits, pair 1(5th,4th)bits, pair 0(4th,3rd)bits.
Compare the encrypted watermark pixel bit pairs with each pixel pair bits of Original image
Watermark
SKC
Encrypted Watermark
Consider each pixel bits and divide into pairs of bits
If there is a matching of bits, then two LSB of the original pixel bits replaced with the assigned number of the respective pair in binary. If there is no matching put the bit pair in the 0th pair and put the pair 00 in two LSB of the respective pixel.
Continue the above process till the end of bit pairs of the encrypted watermark image.
Watermarked Image

Fig. 1. Watermark encoding process.

to 1st pair as (0,1) of the respective pixel of A. If no match is found then compare with 0th pair of pixel of A, If it is a matching then replace the two LSB of the respective pixel of A with the number assigned to 0th pair as (0,0). If no match is found then put the binary data pair of W_c at the 0th pair position of the respective pixel of A and the bit pair 00 in two LSB positions of the same pixel's binary value. Continue this process to cover all pixels of A by the pixels of W_c to get the watermarked image.

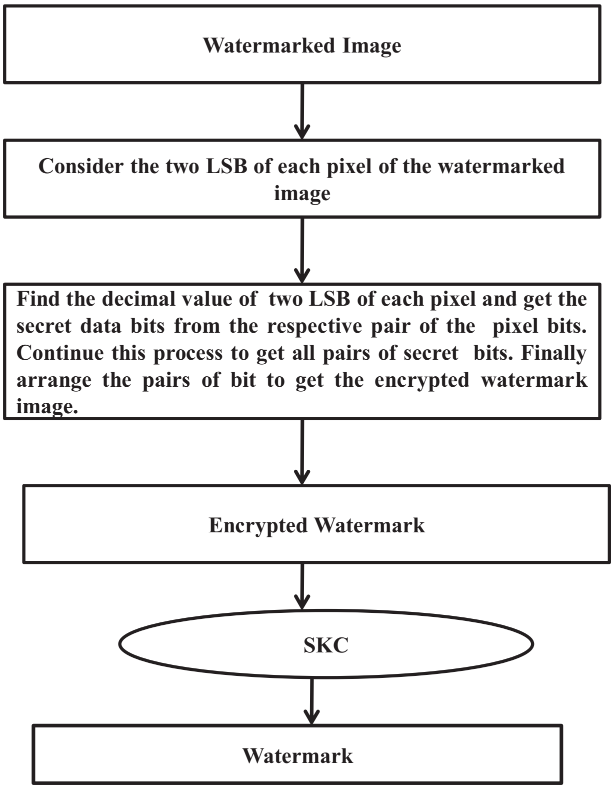

Watermarked Image
Consider the two LSB of each pixel of the watermarked image
Find the decimal value of two LSB of each pixel and get the secret data bits from the respective pair of the pixel bits. Continue this process to get all pairs of secret bits. Finally arrange the pairs of bit to get the encrypted watermark image.
Encrypted Watermark
SKC
Watermark

Fig. 2. Watermark decoding process.

3.3. Decoder

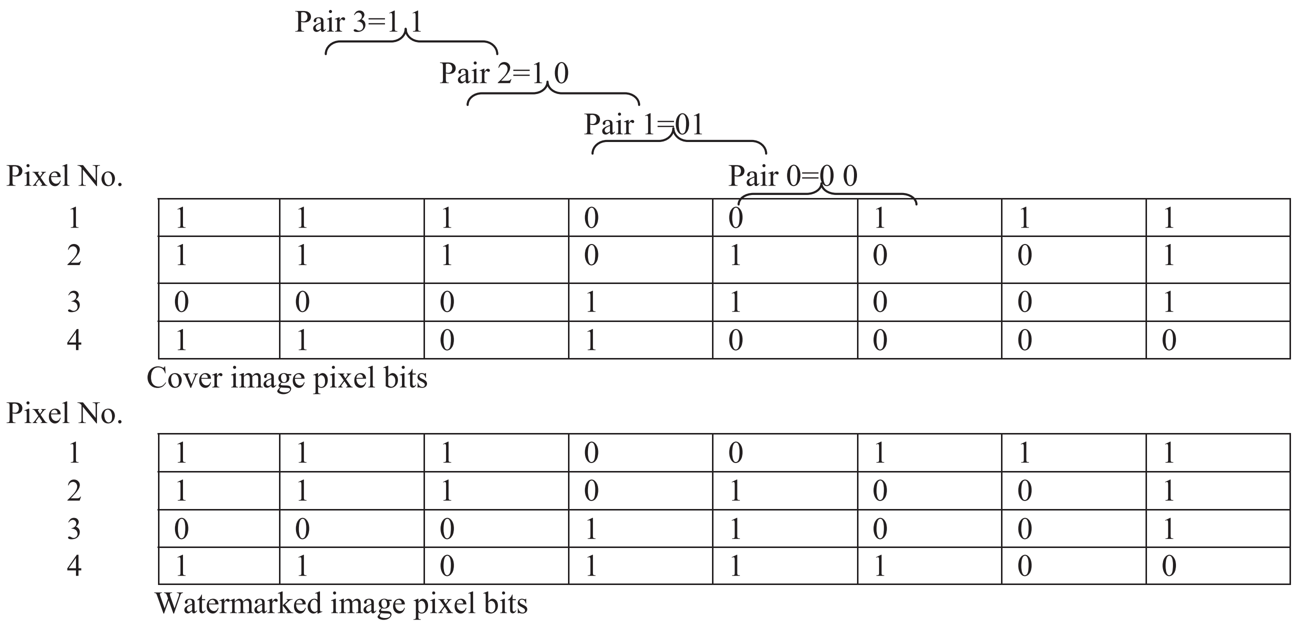
Consider the watermarked image and separate the two LSB bits of each pixel. Then convert LSB bits to decimal value and as per the decimal value, the hidden encrypted watermark data bits can be retrieved from the watermarked image respective pixel's bits pair. Repeat this process for every pixel of the watermarked image and evaluate the secret bits, then arrange the bits to get the encrypted watermark as W_c. Now decrypt the W_c as per algorithm 2 to get the original watermark as B (Fig. 2).

3.4. Encoding process example

Let us encrypt the watermark and consider the encrypted watermark 1st-pixel bits as 11011111. Make the pixel bits into pairs of bits as 11 01 11 11. Let us consider the first four pixel bits of the cover image and bit pairs are given in Fig. 3. Now consider the 1st pair 11 and compare it with 1st-pixel bits pairs of the cover image 11100111. As 3rd pair matched, put the value 11 into the least significant bits of the 1st pixel of the cover image. Now consider the 2nd pair 01 and compare it with 2nd-pixel bits pairs of the cover image 11101001. As 2nd pair matched, put the value 01 into the least significant bits of the 2nd pixel of the cover image. Now consider the 3rd pair 11 and compare it with 3rd-pixel bits pairs of the cover image 00011001. As 2nd pair matched, put the value 01 into the least significant bits of the 3rd pixel of the cover image. Now consider the 4th pair 11 and compare it with 4th-pixel bits pairs of the cover image 11010000. As no match is found, put the pair in the pair 0 and put the pair of 00 at the two LSB positions of the 4th pixel of the cover image. The watermarked image pixels provided in Fig. 3.

3.5. Decoding process example

Consider each watermarked image pixel bits, then separate the two LSB and find out the decimal values. As per the decimal value find out the concern pair bits from the watermarked image pixels. So from the 1st-pixel bits of the watermarked image, the two LSB decimal value is 3, so the bits of the 3rd pair is the encrypted watermark bits pair i.e. 11. From the 2nd pixel bits of the watermarked image the two LSB decimal value is 1, so the bits of the



Pixel No.								
1	1	1	1	0	0	1	1	1
2	1	1	1	0	1	0	0	1
3	0	0	0	1	1	0	0	1
4	1	1	0	1	0	0	0	0

Pixel No.								
1	1	1	1	0	0	1	1	1
2	1	1	1	0	1	0	0	1
3	0	0	0	1	1	0	0	1
4	1	1	0	1	1	1	0	0

Fig. 3. Numerical example of encoding and decoding process.

Please cite this article in press as: Bal, S.N., et al. On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.04.006

1st pair is the encrypted watermark bits pair i.e. 01. From the 3rd pixel bits of the watermarked image the two LSB decimal value is 1, so the bits of the 1st pair is the encrypted watermark bits pair i.e. 11. From the 4th pixel bits of the watermarked image the two LSB decimal value is 0, so the bits of the 0th pair is the encrypted watermark bits pair i.e. 11. So we got 11011111, which are the encrypted watermark 1st-pixel bits.

4. Results and discussion

This segment reflects the proposed method by means of imperceptibility and capacity of data hiding. To judge the performance of the system certain outcomes are assessed with some state of the art mechanisms.

To authenticate the performance of the method, a number of standard grayscale images of size 512 × 512 and one grayscale watermark of size 32 × 32 are used. The grayscale watermark image is given in Fig. 4 and the test grayscale images are given in Fig. 6. To proof, the accuracy of the scheme fifteen sample images is taken for illustration. Below we have given the images with results.

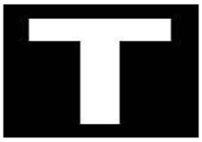


Fig. 4. Grayscale watermark.

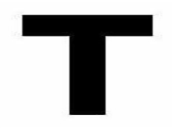


Fig. 5. Watermark after encryption.

The watermark after applying encryption given in Fig. 5 and Fig. 7 shows the watermarked Images.

The encrypted watermark is embedded multiple times within the original grayscale image as per the bit pairs matching using the adaptive bits pair replacement. As the result of embedding, the original image suffers a loss in quality which is calculated by means of some well-known and good quality metrics to check the invisibility of the embedded watermarks for imperceptibility.

4.1. Results of imperceptibility

Fig. 8 shows the bar chart where the original image and watermarked image compared to give the result of imperceptibility.

From the above Fig. 8(i) Mean Squared Error result, all the value lies in between 0.0031 to 0.0034. This confirms less probability of loss of quality.

From Fig. 8(ii) shows the PSNR value for original image verses watermarked image ranged from 51.2948 dB to 52.9925 dB. This indicates achievement of a higher degree of imperceptibility.

Fig. 8(iii) indicates the maximum value for UIQI is one. In the projected method all the values are close to 1(.98 to .99), which indicates the least difference between watermarked image and original image or indicates superior quality.

From Figs. 8(iv) and (v), the structural similarity between the watermarked image and original image are very close and maximum value for both SSIM and MSSIM is approximately 1. In the present mechanism both the values are approaching one for fifteen different images.

4.2. Results of robustness

To show the Robustness of the projected mechanism different attacks like Rotation, Scaling, Crop, Noise Addition, and JPEG

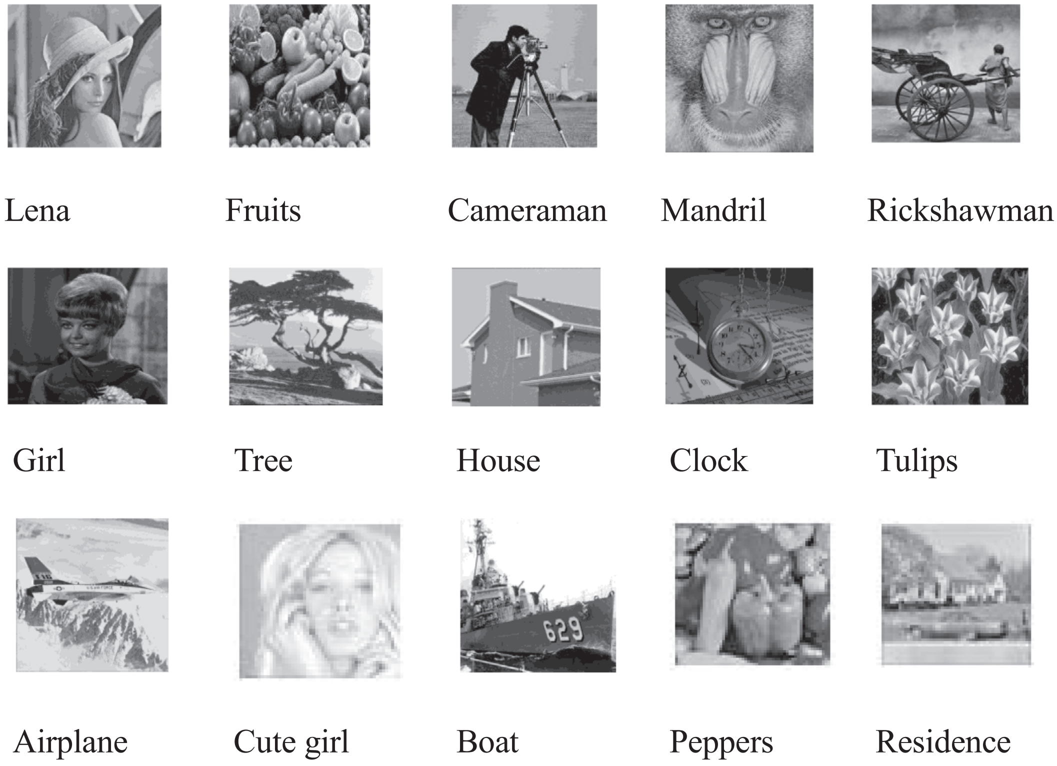


Fig. 6. Original grayscale images.

Please cite this article in press as: Bal, S.N., et al. On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.04.006

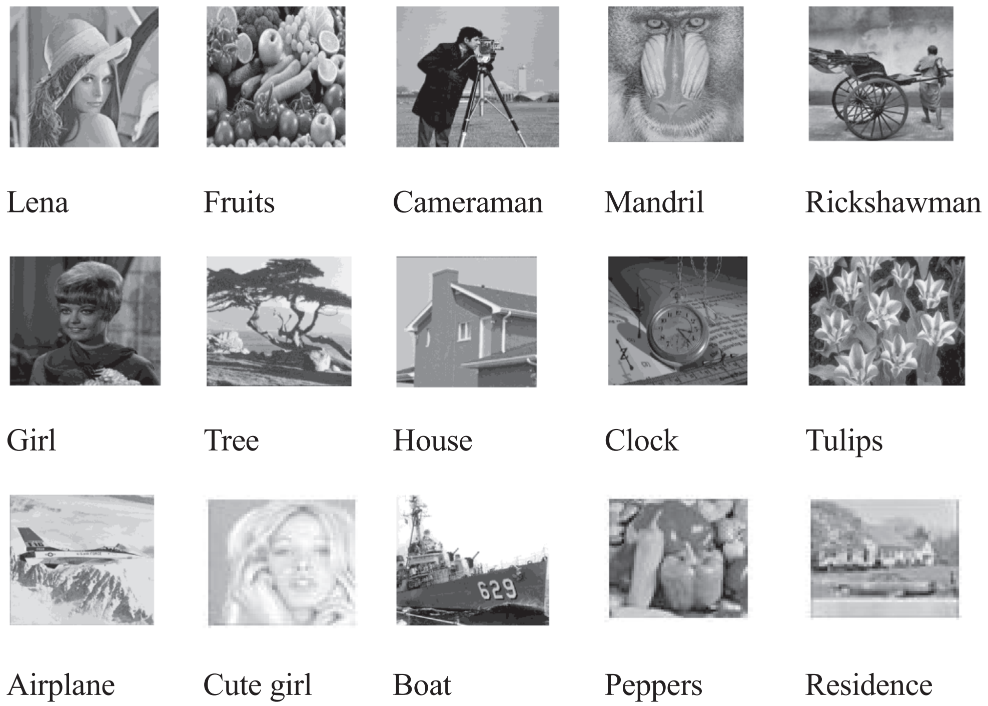


Fig. 7. Watermarked images.

Compression are tested. The bar chart in Figs. 9i–iv shows the outcomes against different kind of impairments, which signifies the revival of the embedded bits and their quality. Here the metrics like Weighted Peak Signal to Noise Ratio (WPSNR), Normalized Cross Correlation (NCC), Similarity measurement (SM), Bit Error Rate (BER) used to show the quality of recovered bits to prove the robustness of the mechanism.

The bit error rate is also very less except Gaussian and Jpeg attacks.

The projected method is robust against most of the unintentional and intentional impairments. The extracted watermarks after different attacks are given below in Fig. 10.

The tool used for all the above experiments is MATLAB 2017 version. It allows the processing of grayscale images for our

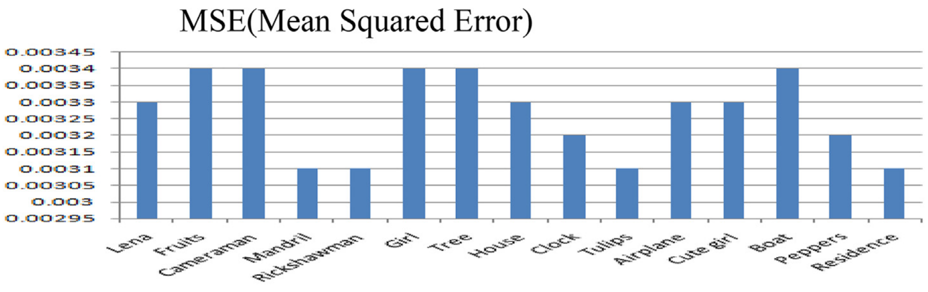


Fig. 8(i). Performance analysis of MSE.

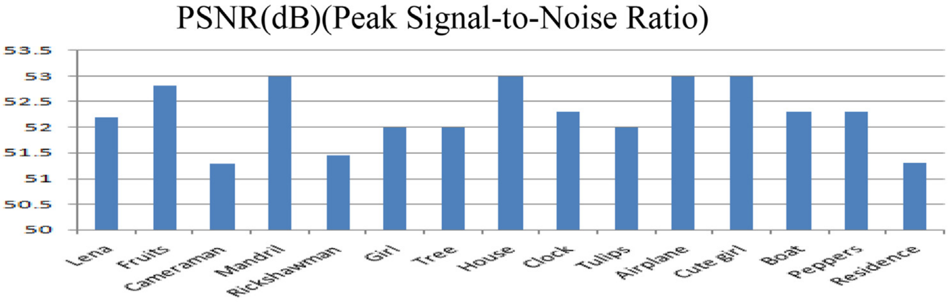


Fig. 8(ii). Performance analysis of PSNR.

Please cite this article in press as: Bal, S.N., et al. On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.04.006

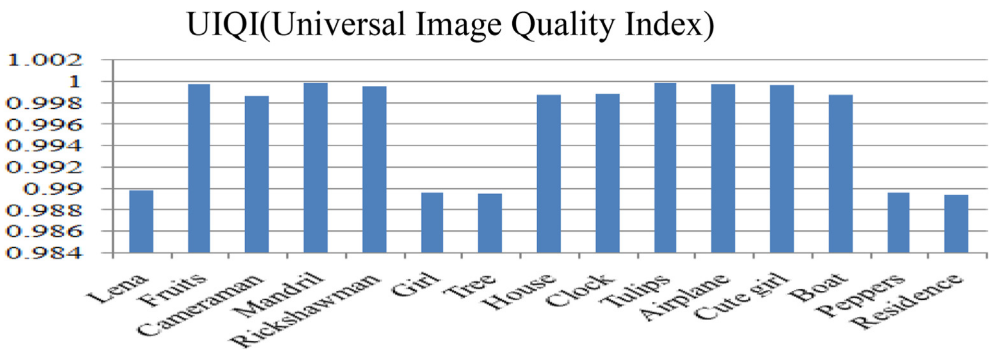


Fig. 8(iii). Performance analysis of UIQI.

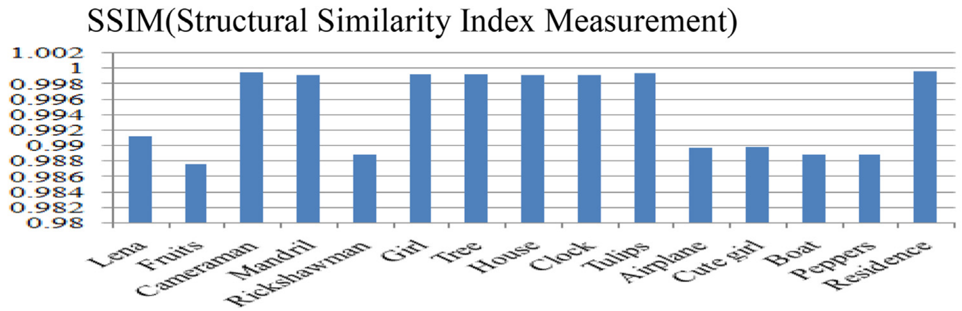


Fig. 8(iv). Performance analysis of SSIM.

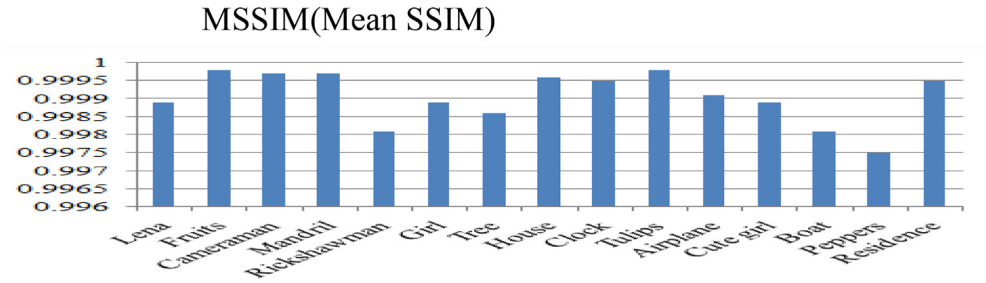


Fig. 8(v). Performance analysis of MSSIM.

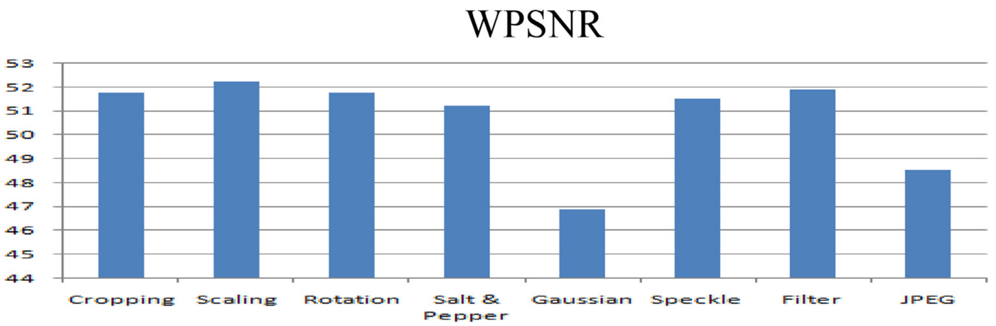


Fig. 9(i). Performance in terms of WPSNR against attacks. Here from the above result, one can check that the value of WPSNR is good for different types of attack and the value is around 52 dB.

purpose of experiments and the coding for the algorithms used in the paper.

To prove the performance of the projected scheme, a comparison among few states of the art algorithms are presented in Table 1. The compared result confirms better imperceptibility and increased capacity of the scheme.

In the proposed scheme fifteen different images are used and the average value is compared with other methods suggested by

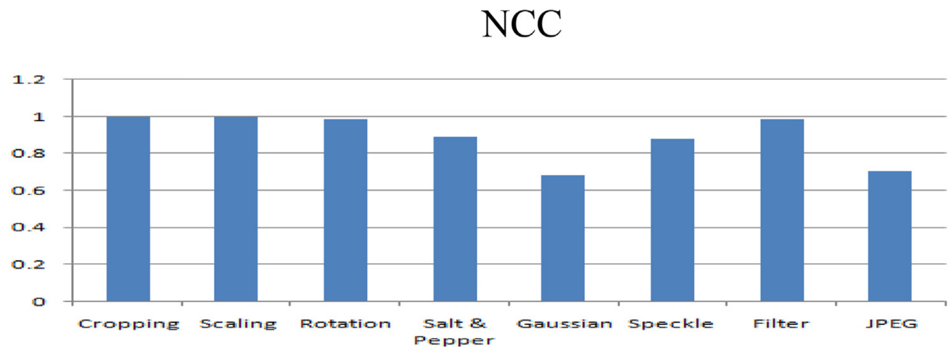


Fig. 9(ii). Performance in terms of NCC against attacks. The above result reflects NCC values are very fine except Gaussian and Jpeg attack.

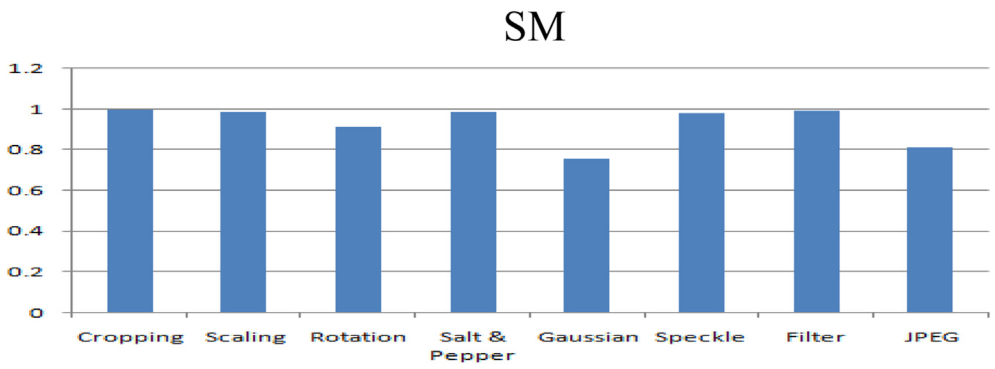


Fig. 9(iii). Performance in terms of SM against attacks. The above chart shows structural similarity values are good and superior.

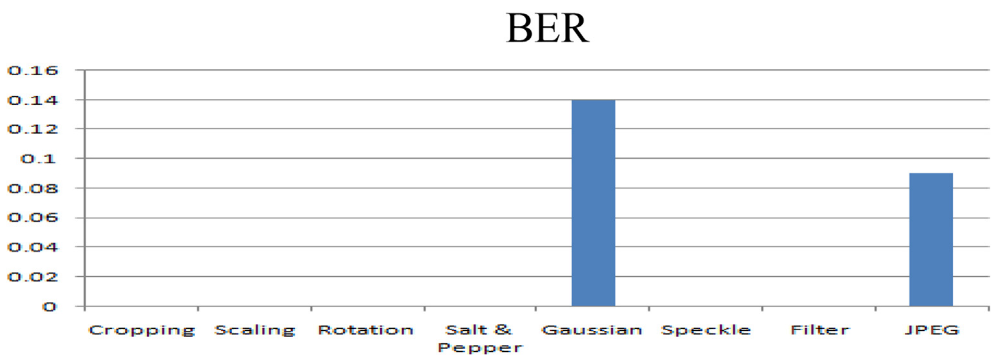


Fig. 9(iv). Performance in terms of BER against attacks.

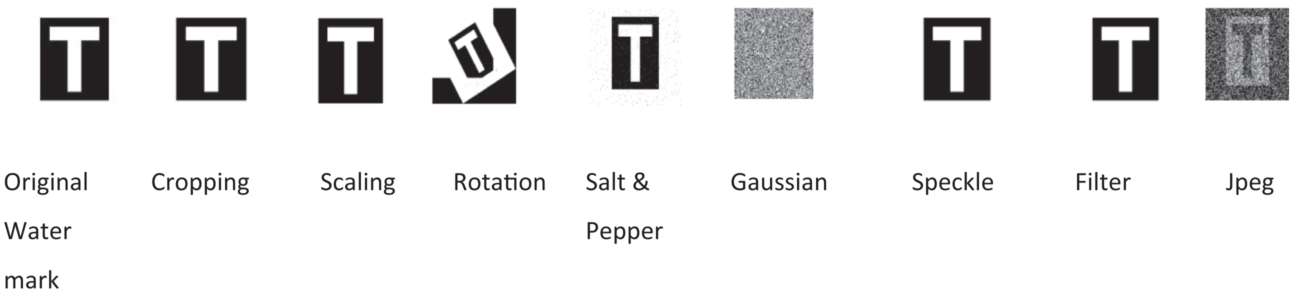


Fig. 10. Recovered watermark after different attacks.

different authors. All the images taken are grayscale in nature and same images are not used for all other algorithms. Therefore, all average results are considered for the comparison process while at the same time maintaining the watermark to record the ratio of payload. In a comparison with the result of others, it is very clear that the proposed method having the highest value of PSNR with the second best payload. This shows that the projected scheme having a higher degree of imperceptibility with the payload.

Please cite this article in press as: Bal, S.N., et al. On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.04.006

Table 1
Comparison of performance results.

Sl. No.	Method	PSNR (dB)	Payload
1	Proposed	52.99	534,266
2	Celik et al. (2002)	38	74,600
3	Nayak et al. (2015)	51.31	249,036
4	Hu et al. (2009)	48.69	60,241
5	Hwang et al. (2006)	48.22	5336
6	Lin and Hsueh (2008)	46.6	59,900
7	Luo et al. (2010)	48.82	71,674
8	Ni et al. (2006)	48.2	5460
9	Vleeschouwer et al. (2001)	39	24,108
10	Wu and Tsai (2003)	41.79	50,960
11	Xuan et al. (2002)	36.6	85,507
12	Yang et al. (2008)	36.28	837,332

5. Conclusions

In this paper bit pairs similarity based LSB replacement watermarking mechanism is proposed. This mechanism is a new concept and which is different from all the previous mechanisms because its main focus is on bit pairs similarity. In this technique to make the watermark more secured, symmetric key cryptography is used and the data bits are arranged in pairs following the proposed scheme, which is different from all the existing techniques. The proposed technique is applied to 15 different grayscale test images. The proposed scheme is more secure, robust and higher payload based on good factors of imperceptibility proved from the results of the experiments we have done.

References

Abu-marie, W., Gutub, A., Abu-Mansour, H., 2010. Image based steganography using truth table based and determinate array on RGB indicator. Int. J. Signal Image Process. (IJSIP) 1 (3), 196–204.

Acken, J.M., 1998. How watermarking adds value to digital contents. Commun. ACM 41 (7), 74–77.

Akhtar, N., 2015. An LSB substitution with bit inversion steganography method. Smart innovation. Syst. Technol. Springer, India 43, 515–521.

Al-Otaibi, N.A., 2014. 2-Leyer security system for hiding sensitive text data on personal computers. Lecture Notes Inf. Theory Eng. Technol. Publishing 2 (2), 151–157.

Al-Otaibi, N.A., Gutub, A.A.A., 2014. Flexible stego-system for hiding text in images of personal computers based on user security priority. In: Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014), Dubai UAE, pp. 250–256.

Altaibi, N.A., Gutub, A.A., Khan, E.A., 2015. Stego-system for hiding text in images of personal computers. In: The 12th Learning and Technology Conference: Wearable Tech/Wearable Learning, Effat University, Jeddah, Kingdom of Saudi Arabia.

Celik, M.U., Sharma, G., Saber, E., 2002. Reversible data hiding. Proc. IEEE Int. Conf. Image Process. 2, 157–160.

Chang, C., Tseng, H., 2004. A steganographic method for digital images using side match. Pattern Recogn. Lett. 25 (12), 1431–1437.

Gutab, A.A.A., Ghouti, L., 2007. Utilizing extension character 'Kashida' with pointed letters for arabic text digital watermarking. In: International Conference on Security and Cryptography (SECRYPT), Barcelona, Spain.

Gutub, A., Al-Qahtani, A., Tabakh, A., 2009. Triple-A: secure RGB image steganography based on randomization. In: The 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-2009), Rabat, Morocco, pp. 400–403.

Hannigan, B.T., Reed, A., Bradley, B., 2001. Digital watermarking using improved human visual system model. In: Ping Wah Wong, Edward J. Delp (Eds.), Proc. SPIE. 4314, 468-474, Security and Watermarking of Multimedia Contents III.

Hempstalk, K., 2006. Hiding behind corners: using edges in images for better steganography. In: Proceedings of the Computing Women's Congress, Hamilton, New Zealand, pp. 11–19.

Hu, Y., Lee, H.K., Li, J., 2009. DE-based reversible data hiding with improved overflow location map. IEEE Trans. Circuits Syst. Video Technol. 19, 250–260.

Huang, F., Zhong, Y., Huang, J., 2014. Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm. Lecture Notes Comput. Sci. Springer, Berlin, Heidelberg 8389, 19–31.

Hwang, J., Kim, J., Choi, J., 2006. A reversible watermarking based on histogram shifting. Digital Watermarking, Springer, 348–361.

Jung, K., Yoo, K., 2015. Steganographic method based on interpolation and LSB substitution of digital images. Multimedia Tools Appl. 74 (6), 2143–2155.

Khan, F., Gutub, A.A.A., 2007. Message concealment techniques using image based steganography. In: The 4th IEEE GCC Conference and Exhibition, Gulf International Convention Centre, Manamah, Bahrain.

Khodaei, M., Faez, K., 2012. New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. IET Image Process. 6 (6), 677–686.

Kutter, M., Hartung, F., 1999. Image watermarking techniques. In: Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information.

Li, B., He, J., Huang, J., Shi, Y., 2011. A survey on image steganography and steganalysis. J. Inf. Hiding Multimedia Signal Process. 2 (2), 142–172.

Li, X., Yang, B., Cheng, D., Zeng, T., 2009. A generalization of LSB matching. IEEE Signal Process Lett. 16 (2), 69–72.

Lin, C.C., Hsueh, N.L., 2008. A lossless data hiding scheme based on three-pixel block differences. Pattern Recogn. 41, 1415–1425.

Liu, R., Tan, T., 2002. A SVD-based watermarking scheme for protecting riahtful ownership. IEEE Trans. Multimedia 4, 121–128.

Low, S.H., Maxemchuk, N.F., Lapone, A.M., 1998. Document identification for copyright protection using centroid detection. IEEE Trans. Commun. 46, 372–383.

Luo, W., Huang, F., Huang, J., 2010. Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inf. Forensics Secur. 5 (2), 201–214.

Macq, B.R., Pitas, I., 1998. Special issue on watermarking. Signal Process. 66 (3), 281–282.

Mahjabin, T., Hossain, S., Haque, M., 2012. A block based data hiding method in images using pixel value differencing and LSB substitution method. In: Proc. International Conference on Computer and Information Technology (ICCIT). Chittagong. Bangladesh, pp. 168–172.

Mandal, J.K., Das, D., 2012. A novel invisible watermarking based on cascaded PVD integrated LSB technique. Commun. Comput. Inf. Sci. Springer, Berlin, Heidelberg 305, 262–268.

Menezes, A.J., van Oorschot, P.C., Vanstone, S.A., 1996. Handbook of Applied Cryptography. CRC Press, Boca Raton, FL.

Mohanty, S.P., 1999. Digital Watermarking: A Tutorial Review. URL: http://www.csee.usf.edu/smohanty/research/Reports/WMsurvey1999Mohanty.pdf.

Nayak, M.R., Tudu, B., Basu, A., Sarkar, S.K., 2015. On the implementation of a secured digital watermarking framework. Inf. Security J.: A Global Perspective 24 (4–6), 118–126.

Ni, Z., Shi, Y.Q., Ansari, N., Su, W., 2006. Reversible data hiding. IEEE Trans. Circuits Syst. Video Technol. 16, 354–362.

Parvez, M.T., Gutub, A.A.A., 2011. Vibrant color image steganography using channel differences and secret data distribution. Kuwait J. Sci. Eng. (KJSE) 38 (1B), 127–142.

Podilchuk, I.C., Wenjua, Z., 1998. Image adaptive watermarking using visual models. IEEE J. Selected Areas Commun. 16 (4).

Roy, B., Rakshit, G., Singha, P., Majumder, A., Datta, D., 2011. An improved symmetric key cryptography with DNA based strong cipher. Int. Conf. Devices Commun. India 1–5. https://doi.org/10.1109/ICDECOM.2011.5738553.

Sabeti, V., Samavi, S., Shirani, S., 2013. An adaptive LSB matching steganography based on octonary complexity measure. Multimedia Tools Appl. 64 (3), 777–793.

Sharp, T., 2001. An implementation of key-based digital signal steganography. Lecture Notes Comput. Sci. Springer, Berlin, Heidelberg. 2137, 13–26.

Sumathi, C., Santanam, T., Umamaheswari, G., 2014. A study of various steganographic techniques used for information hiding. Int. J. Comput. Sci. Eng. Survey (IJCSES) 4 (6), 9–25.

Swanson, M.D., Kobayashi, M., Tewfik, A.H., 1998. Multimedia data embedding and watermarking technologies. Proc. IEEE 86, 1064–1087.

Tsai, Y., Huang, Y., Lin, R., Chan, C., 2016. An Adjustable interpolation based data hiding algorithm based on LSB substitution and histogram shifting. Int. J. Digital Crime Forensics 8 (2), 48–61.

Vleeschouwer, C.D., Delaigle, J., Macq, B., 2001. Circular interpretation of histogram for reversible watermarking. In: Proceedings of the IEEE 4th Workshop on Multimedia Signal Processing, pp. 345–350.

Wang, C., Li, X., Yang, B., Liu, Lu.C., 2010. A content-adaptive approach for reducing embedding impact in steganography. In: Proc. IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP). Dallas. IX, USA, pp. 1762–1765.

Wang, C.M., Wu, N.I., Tsai, C.S., Hwang, M.S., 2008. A high quality steganographic method with pixel-value differencing and modulus function. J. Syst. Softw. 81, 150–158.

Wu, D.C., Tsai, W.H., 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett. 24, 1613–1626.

Xia, Z., Wang, X., Sun, X., Liu, Q., Xiong, N., 2016. Steganalysis of LSB matching using differences between nonadjacent pixels. Multimedia Tools Appl. 75 (4), 1947–1962.

Xuan, G., Zhu, J., Chen, J., Shi, Y.Q., Ni, Z., Su, W., 2002. Distortionless data hiding based on integer wavelet transform. Electron. Lett. 38, 1646–1648.

Yang, C.H., Weng, C.Y., Wang, S.J., Sun, H.M., 2008. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Inf. Forensics Secur. 3, 483–497.

Zhu, X., Zhao, J., Xu, H., 2006. A digital watermarking algorithm and implementation based on improved SVD. In: Proceedings of the 18th IEEE Computer Society International Conference on Pattern Recognition (ICPR'06).

Sanjeev Narayan Bal received his Master in Computer Science from Berhampur University. Working as a Asst. Prof. at Trident Academy of creative Technology, Bhubaneswar, Odisha. Currently, he is working under the guidance of Prof. Subir Kumar Sarkar, Department of Electronics & Telecommunication Engineering, Jadavpur University, Kolkata. His research interests are in the field of image processing and copyright protection.

Manas Ranjan Nayak received his Master in Computer Science & Engineering from Jadavpur University. Currently, he is working under the guidance of Prof. Subir Kumar Sarkar, Department of Electronics & Telecommunication Engineering, Jadavpur University, Kolkata. His research interests are in the field of image processing and copyright protection.

Prof. Subir Kumar Sarkar received his PhD (Tech) degree from Institute of Radio Physics and Electronics, University of Calcutta. He served Oil and Natural Gas Corporation from 1983 to 1992 as Executive Engineer. During 1992 to 1999 he was associated with Electronics and Telecommunication Engineering Department of Bengal Engineering and Science University as a faculty member. Since 1999 he is associated the same department in Jadavpur University where he is currently a Professor. He was the Departmental Head during 2011 to 2013. He has published five engineering textbooks and more than 450 research papers in national and international journals and conference proceedings. He is senior member of IEEE, life fellow of Institute of Engineers, life fellow of IETE, and a member of other professional bodies. He has organized IEEE-sponsored international conferences as CODIS12 during December 2012 as conference chair. His current research interests include digital watermarking, nano-device modeling and simulation, low power VLSI design, and embedded system design.