An Adaptive Data Hiding Technique for Digital Image Authentication

Sarabjeet S. Bedi, Shekhar Verma and Geetam Tomar *Member, IEEE*

Abstract— **The proposed scheme combines the advantages of cryptographic concept and imperceptibility feature of digital image watermarking in spatial domain. The watermark is first generated based on one-way hash function with the help of user key. Each bit of this new generated watermark is then embedded into respective blocks of the original image, in raster scan order. The embedding is performed by modifying the average value of pixel intensity of each block within a range specified by the contrast value for a given block. This reduces the effects of the modification as perceived by the human eye. The extraction procedure computes and compares the sum of the pixels values for the blocks of the original and watermarked image. The results demonstrates the robustness of scheme against common image processing operations like cropping, modification, low pass filter, median pass filter, scaled down and lossy JPEG compression with various quality index factor. Results also illustrate that the watermark is secure, recoverable and recognizable even after the watermarked image has been tampered, forged and modified by common image processing operations. The comparative study of proposed scheme with existing scheme has also been performed to observe the strength of the scheme.**

Index Terms— **Digital Watermarking (DWM), Joint Photographic Expert Group (JPEG), Message Digest (MD), One-way Hash, Spatial Domain.**

I. Introduction

Many commercial vendors and developers use the Internet to deliver media, and transact business. During transmission of digital data, services such as video on demand, electronic data exchange and online shopping, etc. introduce two problems. One is that these services are vulnerable to easy access [1] by illegal users i.e. insecurity of data contents. The other problem is that these services are easy to copy and redistribute. Therefore these services are liable to unauthorized access [2] and use [3]. To provide content authentication and copy protection of digital data, two complementary techniques are being developed: encryption and watermark. Encryption techniques are used to protect digital data during the transmission from sender to receiver [1]. Since digital images can be easily reproduced, cryptosystems do not completely solve this problem. A second security measures that can compliment encryption by embedding a secret imperceptible signal, a watermark, directly into the original data in such a way that it always remain present even during use [4]. Watermarking cannot by itself prevent copying, modification and redistribution of digital media [5].

Various methods in literature [5, 6] which combine watermarking technique with cryptography tools [7] have been proposed to cure these problems. The scheme in [5] has two phases. In first phase, the position of the image using hash function is calculated and then bit of watermark is inserted in the calculated position. The second phase is deriving watermarking phase. The position of an image is calculated in the same way as used in the embedding watermark phase (first phase) and the bit in the position of the image is retrieved. But the scheme has few problems like collision, which may cause lost of some bits of watermark. The other problem is that the position may be chosen in the Most Significant Bit (MSB) of a pixel, which could make the embedded watermark image significantly cloudy, referred as resolution problem.

Another method [6] describes the embedding of watermark in original image by the modification of Least Significant Bit (LSB) with the use of hash function. The secret key and public key are utilized for the content authentication. The scheme is cryptographically secure and provides detection of the location of modification. However, watermarking techniques cryptographic tools have few limitations. The use of LSB to insert watermark is not capable of with standing normal image processing operations like scaling, rotation, modification. The removal and distortion of LSB is easy. A three dimensional representation of LSB is required to represent the LSBs of block, but this increases the required computation. These schemes are useful for content authentication only. Therefore, a scheme is required to fulfill the existing gap in the use of watermarking and cryptographic techniques together.

The proposed scheme combines the advantages of security feature of cryptography, and imperceptibility feature of digital image watermarking. The scheme is concerned with copyright protection, content authentication, security and robustness. The content authentication and copyright protection with robustness of digital still images are achieved by using the features of watermarking in spatial domain where as the security of the scheme is addressed through cryptographic one-way hash function. The paper is organized in six sections. Review of literature and issues of watermarking in spatial domain are discussed in section 2. Section 3 elaborates the watermark embedding and extraction

Manuscript received August 9, 2009.

First author, Sarbjit Singh Bedi is with department of Computer Science and Engineering, M.J.P. Rohelkhand University, Bareilly-243006, India. (e-mail: erbedi@ yahoo.com).

Second author, Shekhar Verma is with Department of Computer Science and Engineering, Indian Institute of Information Technology, Allahabad 211011, India. (e-mail: sv.iiitm@gmail.com).

Third author, Geetam Singh Tomar was with Vikrant Institute of Technology & management, Indore India. Now He is with Malwa Institute of Technology & Management, Gwalior, India as Principal and Machine Intelligence Research Laboratories, India Section, Gwalior, 474011 India. (e-mail: gstomar@ieee.org).

process using hash function in spatial domain. Section 4 demonstrates the results and discussion. A comparative analysis and simulation to check and establish the efficiency of the proposed technique are described in section 5. Conclusion is given in section 6.

II. Background

Information security aspects come into play when it is necessary or desirable to protect the information during transmission from an opponent who poses a threat to its confidentiality and authenticity [8]. Information security thus includes cryptography, traffic security, and importance of privacy and protection of intellectual property rights. The essence of these lies in hiding information [9]. Digital watermarking is a form of information hiding occurs when some unique information (e.g., trademark, symbol) is imprinted inside of another object.

Digital Watermarking (DWM) is the process of embedding information into digital multimedia contents such that the embedded information (watermark) can be extracted later [9]. The complete digital watermarking system model is described using three basic functional components.

A. Watermark Generation

The generating function fg of watermark data, W, is to be added to the original data, Io depending on watermark data, W and key, k. The key may be used as secret or public type. Therefore watermark generation function can be used to protect the watermark and make it secure for the purpose of authentication. This operation can be represented as: Wg = fg (W , k, Io); Where Wg – generated watermark, fg - generating function, W- watermark data, k – key, Io – Original Image (optional).

B. Watermark Embedding

The insertion function fi embed the generated watermark data, Wg into original data, Io and forms the watermarked data, Xw. The insertion function can modify the original data according to watermark data Wg and key k. The insertion is performed in such a way that modification is perceptually similar to the original data. This allows insertion of controlled amount of "distortion" in the original data that can be represented as, Iw = fi (Io, Wg, k); Where Iw – watermarked image, fi – Insertion function, Io – Original Image, Wg - generated Watermark, k – key (optional).

C. Watermark Extraction

The extraction function, fe extracts the watermark data from received watermarked data I'w with the use of corresponding key, k, and original data, Io. This operation can be represented as, We = fe (Io, I'w, k); Where We – Extracted watermark; fe – Extraction function; Io – Original Image; I'w – received watermarked image k – key.

At the receiver side the received watermarked data, I'w, is to be checked for the existence of watermark data Wg. The received watermarked data, I'w may be the indistinct form of watermarked data Iw. In this regard image quality distortion is measured using Normalized Cross Correlation.

In addition to watermark system model, watermarking system must have a number of requirements, some of the most important of these requirements are: watermark robustness, level of perceptibility and payload capacity. These three requirements of watermark are in conflict to a certain degree. Increasing the payload of a watermark for instance is likely to reduce that watermark robustness or increase the level of perceptibility of that watermark.

Watermark based on imperceptible can be visible or invisible in digital media. A visible watermark is embedded in visual contents of digital media in such a way that they are visible along with the content in viewed [10] while an invisible watermark is designed to be transparent to the observer and detected using signal processing techniques [11].

Depending on robustness, the invisible watermark can be classified into two main categories. A robust watermark is designed to resist attacks that do not seriously affect the quality and value of the image [12]. The second category does not tolerate any tampering that modifies the complete integrity of the image, is named fragile invisible watermark [13].

The watermarking can also be classified on the basis of embedding of watermark in original data. The embedding can be done in different processing domains. One approach is to transform the original image into a transform domain representation and embed the watermark data therein. Discrete Cosine Transform (DCT), Discrete Hartley transform (DHT), Discrete Wavelet Transform, etc. have been used as the methods of data transform. In these methods, the watermark is distributed in overall transform domain of the original data. Once the watermark is embedded, it is difficult to destroy. This renders the watermark robust. The second approach is to directly embed in the spatial domain data i.e. pixel intensity values of the original data. A watermarking method based on the spatial domain, scatters information to be embedded to make the information imperceptible.

D. Watermarking System in Spatial Domain

In spatial domain, the watermark is inserted directly by modifying the pixels intensity values. It is most appropriate for fragile watermarking techniques [14] where the watermark is not robust to image processing operations. Spatial domain watermarking methods have larger capacity i.e. more data can be embedded [15]. Since every pixel of watermark in watermarked image has specific location, therefore it is finest for content authentication.

A watermarking technique in spatial domain must fulfill the following properties.

i. The watermarking system should be able to detect any changes made in a marked image after marking.
ii. Watermarking should not alter the quality of the image in a large extent.
iii. The detector should be able to locate the alteration made to an image.
iv. The watermark should be detectable through the correct key, otherwise it should be noise like.
v. The marking key should be difficult to be extracted from the marked image without the correct key.

Despite the several advantages of watermarking techniques in spatial domain [15, 16], it has limitation of robustness. The watermarking in spatial domain is less resilient to common image processing operations. Therefore make a watermark more secure and resistant to common image processing operations a scheme is required to address the above said issues.

III. Proposed Watermarking Scheme

Watermark generation is an extension of [6] with the consideration of secret key only. The necessary steps required for this process are described below and depicted in flow representation diagram in fig. 3.1.

Step1: Original Image of size (i×j), Ii×j and watermark image of size (m×n), Iwm×n is taken. The original image is gray scale image. A gray scale, binary, compressed image may be chosen for watermark image.

Step2: Watermark image, Iw is divided into blocks, bwr(k×l) of size (k×l), where r denote the rth block of image.

Step3: The original image, Io is divided into independent non-overlapping blocks into following two levels.

- bOHp×q of size (p×q) of Io is referred as high level partition and the size of it is based on size of Iw and calculated as: bOHp×q = Ioi×j / Iwm×n
- bOLr(s×t) of size (s×t) is an another partition of Io referred as low level partition and the size of it is based on size of Iw , which is calculated as: bOLs×t = (Ioi×j / Iwm×n)× bwk×l
- where r indicate the index, rth block in the original image correspond to index denoted in block of watermark image bwr.

Step4: For each block bwr of Iw the hash hrp is computed.

$$H(K, X_{Io}, W_{ro}, H_{Io}, r, g^{m}_{r}) = (h^{1}_{p}, h^{2}_{p}, \ldots, h^{n}_{p})$$

where K is user key consisting of a string of bits, X_{Io} is Image index of I^{o}, W_{ro} is Image width of I^{o}, H_{Io} is Image height of I^{o}, r is Image index (each block of I^{o}, correspond to I^{w}) *and* g^{m}_{r} is mean value of pixel intensity of correspond block of I^{o}. The r and H_{Io} are key input parameter to resist with vector quantization attack.

Step5: The new block for watermark generation is computing by XORing (pixel by pixel exclusive OR operation) of hash (h1p, h2p ,…, hnp,) with block (bw1, bw2,…,bwr,) as bgr(k×l) = bwr⊕ hr;

Step6: Repeat step 5 for all blocks and concatenate it, which forms a new generated watermark image Igm×n of size (m×n)

A. Watermark Embedding

Once the binary watermark is generated, it is inserted into the original image. The pixels are inserted individually into blocks of pixels of the original image, and the insertion is made in a pseudo-random fashion. Each bit of the watermark is embedded into the high level partitioned blocks of the original image in raster scan order. The algorithm takes into account the contrast of each individual $n \times n$ block when embedding each bit in order to reduce the effects of the modifications as perceived by the human eye.

To embed the new generated watermark image I^{g} into original image I^{o}, the local statistics, mean and maximum of the intensities of the pixels in each block b^{h} is computed. The contrast value of each block is taken into consideration so that the perceptual quality of the image shall not very much affect. This contrast value of block is computed as $C_{b}=\max(C_{\min}, \alpha(g_{\max} - g_{\min}))$ where α is constant and $C_{\min}$ is minimal value a pixel's intensity can be modified. Thus, the pixels are modified in a manner that is adaptive to the contrast value of the respective block of pixels.

A single bit of new watermark is embedded into a block, b^{h} of the original image, in raster scan order. If a bit '1' is embedded into a block, the average intensity value of this block will be grater then its average value of intensity in same block of original image. While the average intensity value of the block will be lower then its value in same block of original image, if a bit '0' is embedded. This will produce an invisible watermarked image I^{r} of size (i*j).

The modified pixel using the offset will have a small random noise component, however with a nonzero overall mean value. The random nature of this tuning helps to prevent a visible blocking effect. This also contributes to the robustness of the algorithm to the image filtering processes.

B. Watermark Extraction

The extraction of watermark as shown in fig. 3.2 is very simple process and requires the original image, user key and image index. The sum of intensity values of block of original and watermarked image shall be computed. A decoded bit will be '1' If the sum of the intensity values for the block of the watermarked image is greater then the sum of intensity values for the block of the original image, otherwise the decoded bit will be '0'. The decoded bits are then XORed with hash key. The concatenation of these bits produces extracted watermark of size i*j pixels.

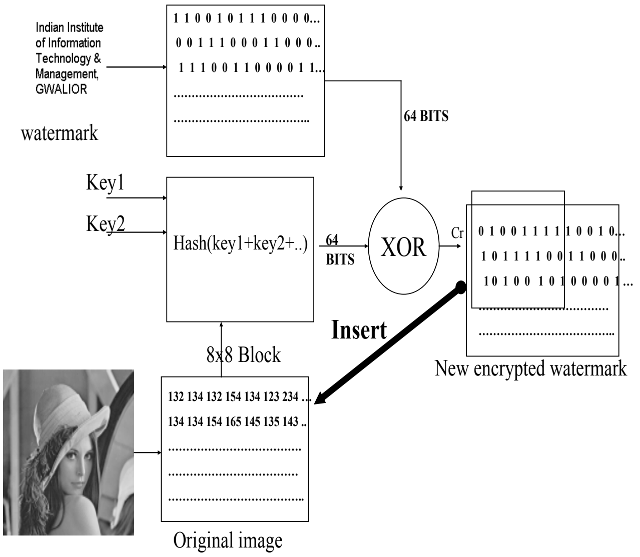


Fig. 3.1: Watermark Generation Process (Flow Representation)

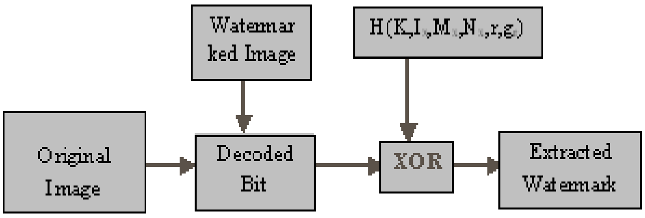


Fig. 3.2: Watermark Extraction Process (Flow Representation)

.

IV. Units

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage. For example, write "15 Gb/cm2 (100 Gb/in2)."

An exception is when English units are used as identifiers in trade, such as "3½ in disk drive." Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength H is A/m. However, if you wish to use units of T, either refer to magnetic flux density B or magnetic field strength symbolized as µ0H. Use the center dot to separate compound units, e.g., "A·m2."

V. Results

This section demonstrates the effectiveness of the proposed algorithm with experimental results and detailed discussion. Several Original gray level images of size 512×512 pixels and watermark images (gray and binary) of size 128×128 pixels with distinguished characteristics are used. The new watermark images of size 128×128 are generated with the use of secret key.

The 64 bit message authentication code (MAC) based on MD5 algorithm for secret key is employed to generate secure watermark images as shown in block diagram of fig. 3.1. The watermark image is divided into blocks of size 8×8 while original image is divided into two levels. The block size of low level is

$$b^{OL} = 512\times512/128\times128 = 4\times4$$

and block size of high level is

$$b^{OH} = (512\times512/128\times128) \times (4\times4) = 32\times32.$$

In this scheme, the extracted watermark is a visually recognizable pattern. The similarity between set of two images like original and watermarked image and another set of two images like watermark and extracted watermark is quantifiably measured by the normalized correlation defined as:

$$NCC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{\sum_i \sum_j \left[W_{ij}\right]^2}$$

Where Wij and W'ij represent the pixel values at location (i,j) in the watermark image and extracted watermark image respectively.

The extraction of watermark and respective correlation values are computed to test the robustness and effectiveness of algorithm.

A. Testing The Security Of Watermark

The first Case is use to demonstrate the localization, adaptive ness and tamper detection ability of algorithm with the use of secret key only.

The original image of Lena is of size 512×512 with 256 gray levels and binary watermark image of size 128×128 as shown in fig. 4.1(a) and fig. 4.1(b) respectively are taken. The user key and image index taken for input are also shown in fig. 4.1(c) and fig. 4.1(d) respectively. The watermarked image of size 512×512 is shown in fig. 4.2(a). The result indicates that watermark is invisible in watermarked image. The use of correct user key for extraction procedure produces extracted watermark image as shown in fig. 4.2(b). While random noise shown in fig. 4.2(c) produces as wrong user key is applied for extraction of watermark. Fig. 4.2(b) and fig. 4.2(c) demonstrate the security of watermark based on hash function and also prove the authentication of image. The NCC value between original and watermarked image is 0.9915 while the NCC value between the extracted and original watermark image is 1.000 obtained.

B. Testing The Robustness Of Watermark (Case-I)

Modification: If the authentic image is tampered by altering certain pixels (modification of the pixel intensity values at specific location) in the watermarked image then the changed areas of the image resembles random noise in corresponding area of extracted watermark. The modification in watermarked image and corresponding extracted watermark are shown in fig. 4.3(a) and fig. 4.3(b) respectively. The computed NCC value between original and modified extracted watermark is 0.9418. Therefore the localization problem is very well addressed in this scheme.

Cropping: Fig. 4.3(c) shows a cropped watermarked image where boarder cropping with different mask size is used. Correspond location of the cropping is shown as random noise in extracted watermark as shown in fig. 4.3(d).

Low Pass Filter: Fig. 4.3(e) shows a linear low pass filtered watermarked image using 3×3 filter mask consisting of 0.9 intensity values. The errors in the watermarked image are still visible at the intensity values changes from a low intensity value to a high intensity value. The extracted watermark from fig. 4.3(e) is shown in fig. 4.3(f), which indicates noise effect as scattered in image. The computed NCC value between watermark image and extracted watermark is 0.8885.

Median Pass Filter: Fig. 4.3(g) shows a Median pass filtered watermarked image using 3×3 filter masks consisting of 0.9 intensity values. The extracted watermark from fig. 4.3(g) is shown in fig. 4.3(h), which indicates noise effect in image. The NCC values between watermark image and extracted watermark is 0.5559. Result shows that scheme resist with median pass filter, where as median filtered image is more blurred than the low pass filtered image.

Scaling Operation: To apply re-sampling operation, the watermarked image is scaled down to one quarter of its original size by using a 2×2 sub sampling operation. The rescaled image is shown in fig. 4.3(i), while the extraction of watermark is shown in fig. 4.4(j). The effect of this operation is more serious as compared to low and median pass filters. The NCC value between extracted watermark and original watermark is 0.4778.

Lossy Compression: To demonstrate the robustness of the scheme, the JPEG compression operation has been performed with the use of various quality factors. The index ranges from 0 to 100 is taken where 0 is best compression and 100 is best quality. The compression ratio for any image is inversely proportional to image quality, i.e. low compression ratio will produce high quality of image, while high compression ratio shall degrade the quality of an image.

The extracted watermark of compressed watermarked image with quality index factor of 90, 80, and 70 are shown in fig. 4.4. The computed NCC value for index-90, 80, 70 and 60 are 0.9309, 0.8452 and 0.7662 respectively.

The combination of various original and watermark images along with watermarked and extracted watermark images has been considered for simulation tests as shown in fig. 4.5.

The graph of NCC values viz. common image processing operations of five test cases is plotted and shown in fig. 4.6. The graph of NCC values viz. lossy JPEG compression quality index factors of five test cases is plotted and shown in fig. 4.7.

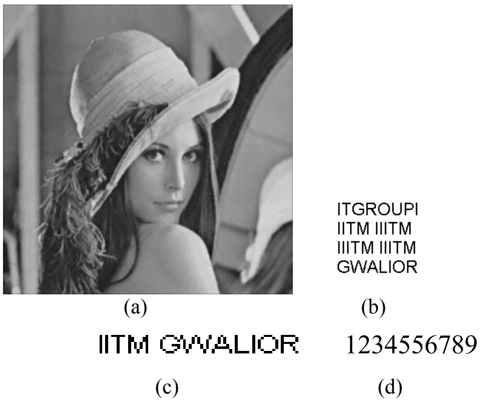


Fig 4.1. (a) Original Gray Scale Image of Lena with size of 512×512 pixels; (b) watermark binary Image of size 128×128 pixels; (c) User Key for Watermark Generation; (d) Image Index for hash function

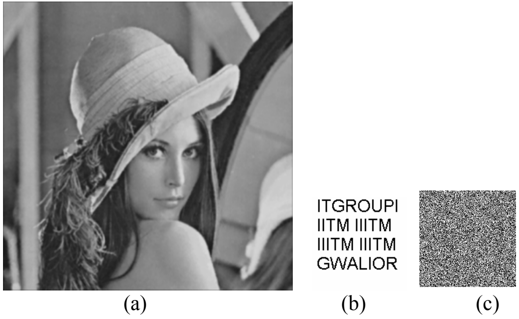
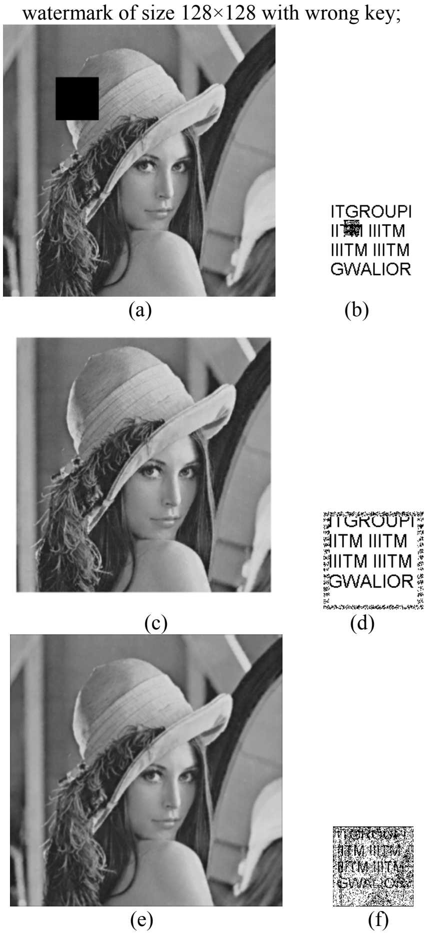


Fig. 4.2. (a) Watermarked Gray Scale Image of size 512×512; (b) Extracted binary watermark of size 128×128 with correct user key; (c) Extracted binary watermark of size 128×128 with wrong key;



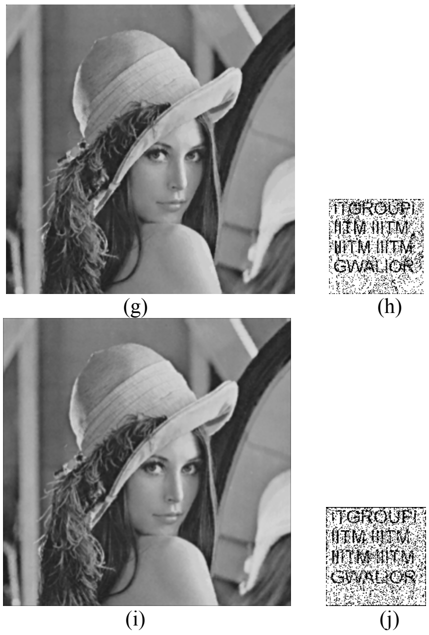


Fig. 4.3. Illustration of some attacks and their effect on extracted watermark: (a) and (b) modification; (c) and (d) cropping; (e) and (f) low pass filter; (g) and (h) Median pass filter; (i) and (j) scale down.

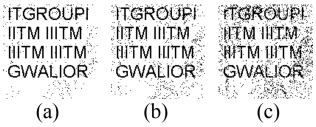


Fig. 4.4. Extracted Watermark Image with JPEG Lossy Compression with various quality factor (QF) index values: (a) QF-90; (b) QF-80; (c) QF-70.

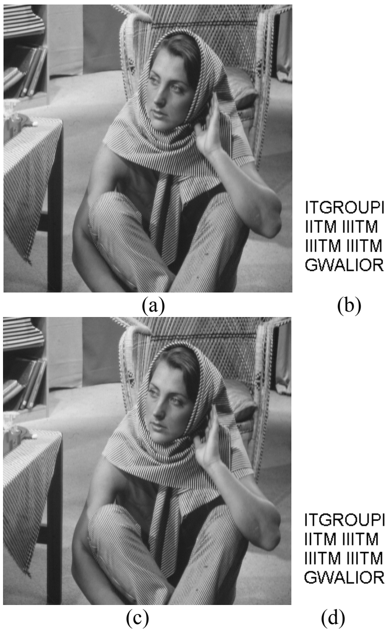
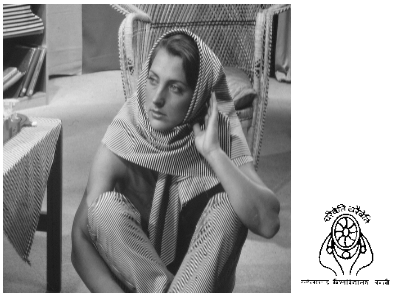
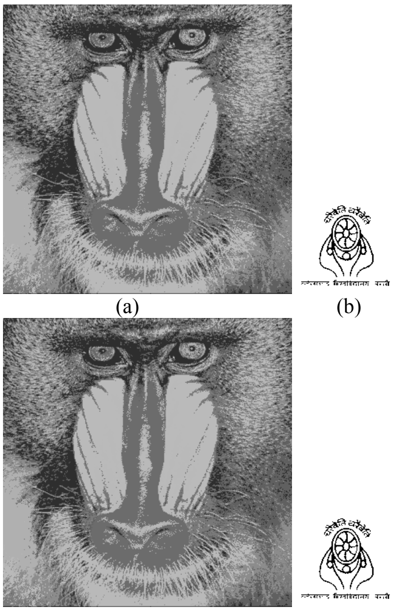


Fig. 4.5. Test Case-II (a) Original Gray Scale Image of Barbara of size 512×512 pixels; (b) Binary watermark image of size 128×128 pixels; (c) Watermarked Gray Scale Image of size 512×512; (d) Extracted binary watermark of size 128×128.



(c) (d)

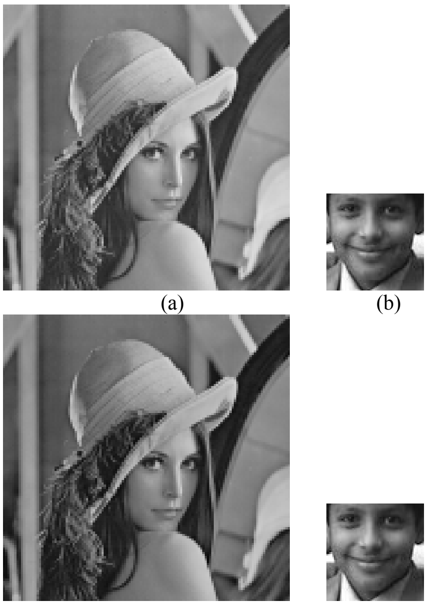
Fig. 4.6: Test Case-III (a) Original Gray Scale Image of Barbara of size 512×512 pixels; (b) Binary watermark image of size 128×128 pixels; (c) Watermarked Gray Scale Image of size 512×512; (d) Extracted binary watermark of size 128×128;



(a) (b)

(c) (d)

Fig. 4.7. Test Case-IV (a) Original Gray Scale Image of Mandrill of size 512×512 pixels; (b) Binary watermark image of size 128×128 pixels; (c) Watermarked Gray Scale Image of size 512×512; (d) Extracted binary watermark of size 128×128.



(a) (b)

(c) (d)

Fig. 4.8. Test Case-V (a) Original Gray Scale Image of Lena of size 512×512 pixels; (b) Gray scale watermark image of size 128×128 pixels; (c) Watermarked Gray Scale Image of size 512×512; (d) Extracted gray scale watermark of size 128×128;

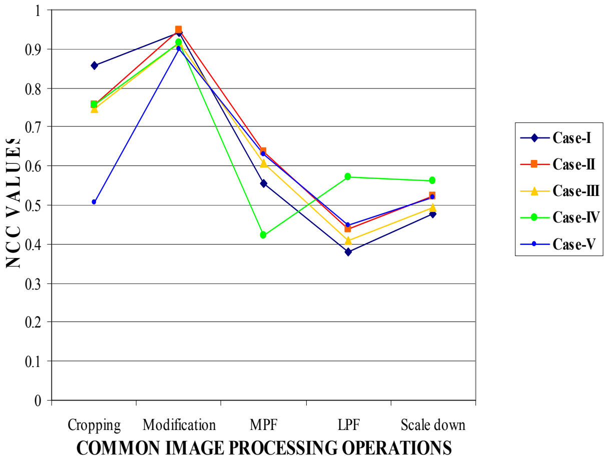


Fig. 4.9. Graph for NCC values of various image processing operations of five test cases of proposed scheme.

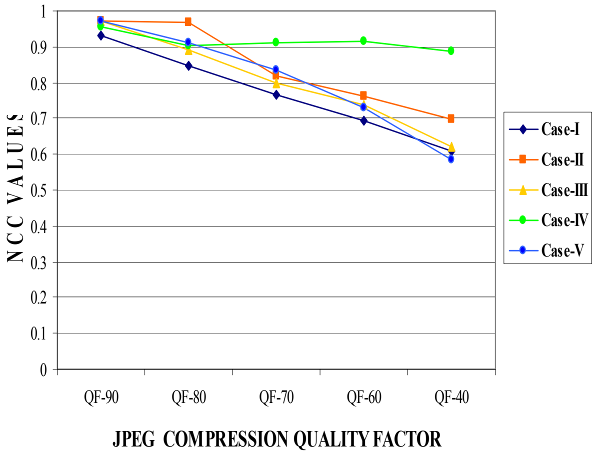


Fig. 4.10. Graph for NCC values of various quality factors of lossy JPEG compression of five test cases of proposed scheme.

VI. Conclusion

The proposed scheme indicates that one who has correct user key can only verify the ownership, while image cannot be tampered with the use of wrong key. The results demonstrated that any modification to watermarked image would be reflected as corresponding error in the extracted watermark. The experimental results demonstrate that the scheme is robust to lossy JPEG compression, low pass filter, scaled down, cropping and rotation, while best results are found in modification, cropping, and median pass filter in respective order. The performance analysis and the strength of the scheme have been compared with a few existing schemes.

It is observed that the watermark is secure, recoverable and recognizable even after the watermarked image has been tampered, forged or modified by image processing operations. The technique is suitable candidate for embedding a secure and robust watermark in an image.

The information rate and the payload capacity of watermarking system are decreases due to the use of cryptography concept. Such limitations needed to be addressed in future work.

REFERENCES

[1] Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source code in C”, John wiley and sons Inc., 2ed ed., USA, 1996, ISBN: 0-471-12845-7.

[2] J. B. Borka, “Security in value added networks security requirements for EDI”, Computer standard & Interfaces, vol. 12, pp. 23-33, 1991.

[3] I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia”, IEEE Transaction on Image Processing, vol. 6, pp. 1673-1687, 1997.

[4] S. Juergen, “Digital watermarking for digital multimedia”, Information science Publishing, USA, 2005, ISBN: 1-59140-520-3 (ebook).

[5] Hwang, and Min-Shiang, “A Watermarking Technique Based on One-Way Hash Functions”, IEEE Trans on Computer Electronics, vol 45, pp. 286-294, May 1999.

[6] PP. W. Wong, and N. Memon, “Secret and Public key Image Watermarking Schemes for Image Authentication and Ownership Verification”, IEEE Transaction on Image Processing, vol. 10, no. 10, Oct. 2001.

[7] William Stallings, “Cryptography and Network Security: Principles and Practice”, Third edition, Pearson Education India, 2003, ISBN: 8178089025.

[8] Wayner Peter, “Disappearing Cryptography”, Information Hiding, Steganography and Watermarking, Second Ed., Morgan Kauffmann Publishers, 2002.

[9] C. Y. Lin and S. F. Change, “Multimedia Authentication”, Proceeding of SPIE-International Conference on Security and Watermarking of Multimedia Contents. http://www.ctr.columbia.edu/~cyhh/auth/mmauth.html.

[10] H. Sencars, M. Ramkumar, and A. Akansu, “Digital Hiding Fundamental and applications”, Elsevier Academic Press, San Diego, CA, 2004. ISBN: 0-12-047144-2.

[11] S. Juergen, “Digital watermarking for digital multimedia”, Information science Publishing, USA, 2005, ISBN: 1-59140-520-3 (ebook).

[12] J. J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann,, “Lecture Notes in Computer Science, eds. Computer Security”, 5th European Symposium on Research in Computer security, ESORICS-1998, Belgium, vol. 1485, Sepp. 1998, ISBN 3-540-65004-0.

[13] K. Tanaka, Y.Nakamura, and K. Matsui, “Embedding secret information into a dithered multilevel image”, Proceeding of IEEE Military Comm. Conference, pp.216-220, Sept. 1990.

[14] PP.S.L.M. Barreto, H.Y. Kim, and V-Rigmen, “Toward seeure public key blockwise fragile authentication watermarking”, Proc of IEEE Magz., vol. 149, no. 2, pp. 57-62, April, 2002.

[15] F.Hartung and M.Kutter, “Multimedia watermarking techniques”, Proceeding of IEEE Conference, vol. 87, pp. 1079-1106, July 1999.

[16] M.Yeung, I. Mintzer, “Invisible watermarking for image verification”, Journal of Electric imaging, vol. 7, no.3, pp. 578-591, July 1998.

[17] S.-C. Hsia, I.-C. Jou, S.-M. Hwang, “A gray level watermarking algorithm using double layer hidden approach”, IEICE Transaction on Fundamentals of Electronics, Communications and Computer Science E85-A, vol. 2, pp. 463– 471, 2002.

[18] Jian Reu, Tongtong Li, M. nadoosham, “A Cryptographic Watermarking Embedding Technique”, IEEE, 0-7803-8622-1/04/$20.00, 2004.

Sarabjeet Singh Bedi received the M.E. degree in Computer Science and Engineering from Thapar Institute of Engineering and Technology, Punjab, India in 2002. His Ph.D. Thesis is submitted at Indian Institute of Information Technology and Management, Gwalior, India. He has teaching and research experience of 13 years. His research interest is Network Management and Security. Currently He is teaching at M.J.P. Rohilkhnad University, Bareilly, India. He is involved in various academic and research activities. He is member of selection, advisor, governing and technical committees of various Universities and Technical Institution bodies. Mr. Bedi received Institute Medal from TIET, Punjab, India, 2002 and Rastriya Shikshak Ratan Award from AIBDA, New Delhi in 2002.

Geetam Singh Tomar (IEEE M’02), received B.Tech, M.E. and Ph.D. degrees from reputed universities of India. He is currently involved in many research projects and consultancies through MIR Labs (USA), India section. Currently he is with Malwa Institute of Technology and management, Gwalior as principal. He has more than 21 years of professional experience and is actively involved in IEEE conferences all over the world. He is editor of two international Journals and Chief editor of two international journals. Presently he is conference chair of five IEEE conferences in Asia.