Volume 6, Issue 2, April-September 2015

ISSN: 0973-7391 Impact Factor: 2.5 Available at www.csjournals.com

International Journal of Computer Science & Communication

A Novel Watermark Approach for securing Fingerprint Template

Rubal Jain[1], Arun Kumar Yadav[2], Dr. Chander Kant[3]
[1,2] Research Scholar, Department of Computer Science and Applications, K.U., kurukshetra, INDIA
[3]Asst. Professor, Department of computer Science and Application, K.U., Kurukshetra, INDIA
rubaljain.92@gmail.com, ckverma@rediffmail.com

Abstract: In the present scenario, data security is one of the major challenges. Watermarking is a technique in which a digital signal or pattern is inserted into a digital image for security reasons. Watermarking is mainly used for copyright protection, owner authentication and id card security. A watermark is a signal added to digital data such as audio, video and still images that can be detected or extracted later. The existence of such a watermark can be determined only through a watermark extraction or detection algorithm. In general, watermark can be embedded in Spatial domain or Transform domain. The digital watermarks suffer from different types of attacks that include either state-of-the-art watermarking attacks or watermark estimation attacks. The recovery from these attacks requires strong detection techniques. In this paper, the author proposes a new watermarking algorithm which is based on the existing LSB algorithm. The proposed watermarking algorithm embeds watermark text into the fingerprint template. It is based on the concept of one's complement the watermark bit before it is embedded which is decided on the basis of MSB of pixel value in which watermark bit is to be embedded.

1. Introduction

Digital Watermarking is a technique in which pattern of bits are inserted into a digital image, audio or video file that indicates the file's copyright information such author, rights and so on [1]. Thus, watermarking approach is used to make sure of the protection of the data. However, watermarking is also designed to be completely invisible. The actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be detected and tampered [2]. Thus, the watermarking must be robust enough so that it can withstand normal changes to the file such as attacking by adding noise. Contrast to printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that is completely invisible. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data [3]. Media watermarking research is a very active area and digital image watermarking became an interesting protection measure and got the attention of many researchers since the early 1990s [4] .

1.1 Attacks on Digital watermarks

Attacks on digital watermarks are categorized to either state-of-the-art watermarking attacks or watermark estimation attacks [5].

i. State of the art watermarking attacks

This category of attacks includes four types of attacks that are removal attacks, geometric attacks, cryptographic attacks, and protocol attacks.

- **Removal attacks:** Removal attacks target at the removal of watermark information completely from the watermarked data without breaching the security of the watermarking algorithm, e.g., without the key used for watermark embedding. This category of attacks includes

denoising, quantization (e.g., for compression), demodulation, and collusion attacks'. These attacks might not be able to complete their aim of removal of the watermark completely but they may destroy the watermark information.

• **Geometric attacks:** In contrast to removal attacks, geometric attacks are not interested in the removal of the watermark but they aim to distort the watermark detector synchronization, embedded with the information. This detector could be used to recover the embedded digital watermark information when perfect synchronization is regained, but in terms of practical situations this process is very expensive and very complex.

• **Cryptographic attacks:** Cryptographic attacks intend to breach the security algorithm used to embed the watermark, and thus finds the way to remove the embedded watermark or to embed misleading watermarks. An example of this type of attack is brute force attack and Oracle attack which are used to generate a non watermarked signal.

• **Protocol attacks:** The main target of Protocol attacks is to damage the watermark application entirely. An attack based on invertible watermarking is an example of this type. In this case the attacker extracts the watermark from the watermarked data claiming the ownership of this watermarked data. It results in ambiguity with respect to the true ownership of the data.

ii. Estimation based attacks

These attacks require a well knowledge in watermarking technology and the characteristics of the data. The main concept of these attacks is that the original data or the watermark can be estimated by the attacker because the attacker has previous knowledge of the watermark signal statistics. The estimation based attacks can be classified into removal attacks, protocol attacks, or de-synchronization attacks [5].

• **Estimate of the original data:** The watermark is an addition to the original data; the attacker can design an extraction technique to get the unwatermarked data. The extraction technique depends on both denoising and compression of the watermarked signals. The denoising and compression attacks are classified as removal attacks.

• **Demodulation attacks:** Demodulation attacks modifies the watermark by using an opposite technique of the embedding algorithm used with the original data, if an approximate estimation is made to the real watermark then the estimated watermark can be subtracted from the original watermarked data which may affect the original data quality.

• **Copy attack:** The estimated watermark can be used in a copy attack implementation. The attacker adds the estimated watermark to a target data claiming the ownership of the falsely watermarked data.

• **Synchronization removal:** The synchronization removal attack depends on detection of the synchronization mechanisms used with the original data then removing the synchronization and applying desynchronization techniques. By this important characteristics of the original data is extracted, which make it easy to get the original data.

The rest of this paper is organized as follows: Section 2 describes the related work to digital watermarking. Section 3 discusses the proposed method and also contains sub-sections. Section 3.1 provides a working of the proposed method and section 3.2 describes proposed watermarking algorithm. Finally section 4 concludes the paper along with the future scope of the digital watermarking.

2. Related Work

The two fundamental approaches to embed data in a binary image are by modifying the values of individual pixels and by modifying a group of pixels [6]. The first approach used for data hiding in binary image simply toggles a white pixel to black or vice versa, whereas second approach modifies some elements such as thickness of strokes, relative position etc. The rapid increase of interest in watermarking the objects is most likely due to the raise in concern over copyright protection of content. The former technique used for protecting the ownership of multimedia objects is cryptography, where encryption is followed by decryption. But nowadays watermarking has been investigated as a complementary technology. Digital watermarking is the most widely used approach for embedding watermarks in multimedia objects and has been extended from still images to video [7]. In general, watermark can be embedded in Spatial domain or Transform domain. There various approaches comes under the category of spatial domain technique are LSB Correlation-Based, Patchwork, Random function, Image checksum, M frame, SST, and Kodak Technique. For Transform Domain approaches available are DCT, DWT, DFT, SST, Continuous Transform and Random [8]. Hao Luo et al [9], presented the idea of self-embedding watermarking scheme for digital images. In proposed algorithm, the author transform the host image to a halftone image and this halftone image is used as compressed version of the host image and further adopted as a watermark. Then, the watermark is pixel wise permuted and embedded in the LSB of the host image. The watermark is retrieved from the LSB of the suspicious image and inverse permuted. On the other hand Wen-Chao

Yang et al [10] used the PKI (Public-Key Infrastructure), Public-Key Cryptography and watermark techniques are used to design a novel testing and verifying method of digital images. The idea of the author is to embed encryption watermarks in the least significant bit (LSB) of digital images. The advantage of designed method is that the integrity of digital images can be checked. Hong Jie He et al [11], proposed a wavelet-based fragile watermarking scheme for secure image authentication. In this paper, they generated the embedded watermark using the discrete wavelet transform (DWT), and then they elaborated security watermark by scrambling encryption is embedded into the least significant bit (LSB) of the host image. Sung-Cheal Byun et al [12], presented the idea of a fragile watermarking scheme for authentication of images. The author utilizes singular values of singular value decomposition (SVD) of images to verify the integrity of images. In order to make authentication data, the singular values are changed to the binary bits using modular arithmetic. Then, they inserted the binary bits into the least significant bits (LSBs) of the original image. The pixels to be changed are randomly selected in the original image. Gil-Je Lee et al [13] presented a new LSB digital watermarking scheme by using random mapping function. The idea of their proposed algorithm is embedding watermark randomly in the coordinates of the image by using random function to be more robust than the traditional LSB technique. Saeid Fazli et al [14] presented trade-off between imperceptibility and robustness of LSB watermarking using SSIM Quality Metrics. In their algorithm, they put significant bit-planes of the watermark image instead of lower bit-planes of the asset picture. Debjyoti Basu et al [15] proposed Bit Plane Index Modulation (BPIM) based fragile watermarking scheme for authenticating RGB color image. By embedding R, G, B component of watermarking image in the R, G, B component of original image, embedding distortion is minimized by adopting least significant bit (LSB) alteration scheme. Their proposed method consists of encoding and decoding methods that can provide public detection capabilities in the absences of original host image and watermark image.

The above section of related work gives idea that there is some issues with all the existing techniques. There is no full-proof approach which is capable to resist watermark attacks. In following section 3, the author would also like to introduce a new alternative technique by inserting watermark text in grayscale images by using watermarking approach. Although the proposed technique is also not full-proof but may help in overcoming the drawbacks of existing LSB based approaches.

3. Proposed Method

The framework of the proposed method formulates about providing security to the fingerprint template of an individual along with the use of well known template protection scheme known as digital watermarking. The author proposes a new watermarking algorithm which is based on the existing LSB algorithm and provides security to maintain integrity and confidentiality of the fingerprint template. The framework of the proposed method is shown in fig.1 which illustrate that method is capable of embedding watermark in the fingerprint template as well as to retrieve watermark from the fingerprint template.

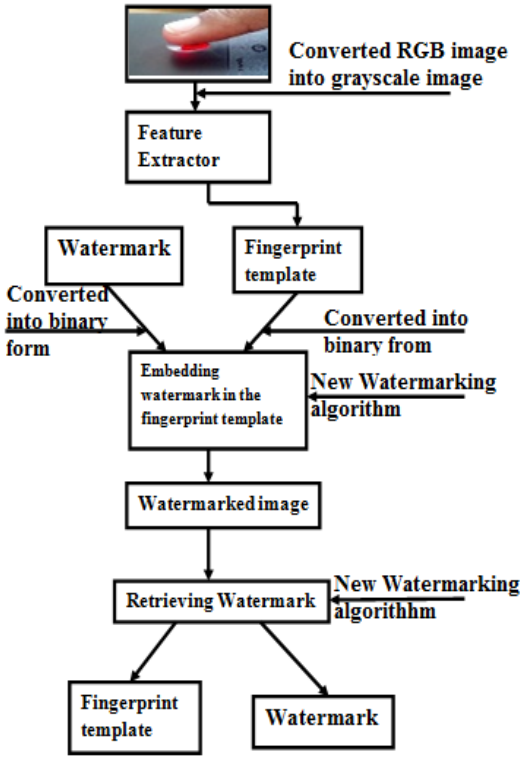

Fig.1 Framework of the Proposed Method

3.1 Working of the proposed method

1. The sensor is used to acquire fingerprint image and this image is in RGB pixel format.

2. Convert the RGB image into grayscale image. Each image file in grayscale pixel format contains 8-bits per pixel.

3. After converting to grayscale image then image is preprocessed including enhancement, binarization, denoising and ridge extraction.

4. From preprocessed image necessary features are extracted (e.g., minutiae) which generates the fingerprint template.

5. Convert the fingerprint template into its binary equivalent from decimal equivalent.

6. Select the watermark text which will be embedded into the fingerprint template and convert it into a binary form.

7. After converting to binary form, embed the watermark text into the fingerprint template with the help of steps for watermark embedding described in the proposed

watermarking algorithm which results in watermarked image.
8. For retrieving the watermark, watermarked image is used as input and by applying watermark extraction steps on it, described in proposed watermarking algorithm watermark will be retrieved.
9. After retrieving the watermark it can be compare with the original watermark. If any distortion is found then there are chances of malicious attacks on watermark caused by intruders.

3.2 Proposed Watermarking Algorithm

The proposed watermarking algorithm is based on the existing LSB algorithm. The idea of proposed algorithm utilizes the concept of 1's complement of the watermark bit. It is decided on the basis of the value of MSB of the current pixel whether to complement the watermark bit or not. In this way a new approach of embedding watermark is proposed where MSB's of the pixel values of fingerprint template is used for embedding as well as retrieving the watermark.

Steps for data embedding

1. Convert the acquired fingerprint image from RGB image to grayscale image and find the number of pixels (p1, p2, p3……pm). Each grayscale image has 8-bits per pixel.

2. Convert the grayscale image into binary form.

3. Convert the watermark text into binary equivalent and store it in the form of 1-D array. Here the size of watermark text must be much smaller than the size of fingerprint image. The number of bits (b0, b1, b2……. bn) in watermark text must be much smaller than number of pixels (p1, p1, p2…….pm) of grayscale image. Hence, n<m.
4. For embedding purpose, INITIALIZE [PIX=1], INITIALIZE [B=0]. Here PIX refers to pixel number of base image or cover image and B refers to the number of bit in the watermark text which is stored in the form of 1-D array.
5. For [B=0 to n]
{
For [PIX= 1 to n]
{
if (MSB=1)
{

Then

a. 1's complement of the value of current watermark bit is stored in most LSB of the current pixel of base image.

}
Else
{
a. Actual Value of current watermark bit is stored in the most LSB of the current pixel of base image.
}
}
PIX++;
B++;
}
6. After step 5th, the modified base image is known as watermarked image.

Steps for watermark extraction

1. Read the watermarked image.
2. For retrieving watermark from the watermarked image, INIT [PIXL=1]. Here PIXL refers to the number of pixel in watermarked image.
3. For [PIXL=1 to n]
{
If (MSB=1)
{

Then
a. 1's complement the most LSB of the current pixel of watermarked image and then store it in 1-D array.
}
Else
{
a. Actual value of the most LSB of the current pixel of watermarked image is stored in 1-D array.
}
PIXL++;

}

4. After step 3rd receiver is able to retrieve the fingerprint template and watermark text in binary form.
5. Convert the fingerprint template and watermark text from their binary equivalent to decimal equivalent.
6. After step 5th watermark text is extracted in its original form and fingerprint template is obtained as grayscale image.
7. Convert the fingerprint image from grayscale pixel format to RGB pixel format.

4. Conclusion and Future Scope

The idea is to embed the watermark text into the grayscale fingerprint image. These watermark text are not embedded into the whole fingerprint image. Instead they are embedded into specific regions of fingerprint image. The proposed watermarking algorithm which is based on existing LSB algorithm has been chosen for embedding the watermark text into the fingerprint image. It is a less robust watermarking technique, but since we have focused on large capacity, it seemed to be less important. Since we replaced only the last bit of the cover image data with the watermark data, the imperceptibility of the watermark is

pretty high. The future work may focus on more robust and larger capacity. Although there is contradiction between these two aspects but it could be solved with a balance solution according to the practical application. The idea of embedding watermark may be extended to the video application area. Using multimedia Object for embedding watermarks is a pretty new concept and with the passage of time, it will gain more and more attention. In future, it may also be possible to identify additional platforms for embedding watermarks apart from the traditional platforms such as image, audio, video.

References

[1] R. Goyal and N. Kumar, "LSB Based Digital Watermarking Technique," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 9, pp. 15-18, September 2014.

[2] C. Serrao and J. Guimaraes, "Protecting Intellectual Proprietary Rights through Secure Interactive Contract Negotiation," vol. 1629, Springer-Verlag Berlin Heidelberg, 1999, pp. 493-514.

[3] S. Katzenbeisser and F. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, London: Artech House , 2000, p. 240.

[4] A. Bamatraf, R. Ibrahim and M. N. M. Salleh, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit," JOURNAL OF COMPUTING, vol. 3, no. 4, pp. 1-8, april 2011.

[5] H. H. Nasereddin, "Digital Watermarking A Technology Overview," IJRRAS , vol. 6, no. 1, pp. 89-93, January 2011.

[6] Y. Y. C. Y. C. Tseng, "A Secure Data Hiding Scheme for Binary Image," IEEE Transc. On Communication, vol. 50, no. 8, pp. 1227-1231, August 2002.

[7] J. Hussein and A. Mohammed, "Robust Video Watermarking using Multi-Band Wavelet Transform," International Journal of Computer Science Issues (IJCSI), vol. 6, no. 1, pp. 44-49, 2009.

[8] P. Singh and R. S. Chadha, "A Survey of Digital Watermarking Techniques,Applications and Attacks," International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, no. 9, pp. 165-175, March 2013.

[9] H. Luo, S.-C. Chu and Z.-M. Lu, "Self Embedding Watermarking Using Halftoning Technique," Circuits,Systems and Signal Processing, vol. 27, no. 2, pp. 155-170, April 2008.

[10] C.-Y. W. C.-H. C. Wen-Chao Yang, "Applying Public-Key Watermarking Techniques in Forensic Imaging to Preserve the Authenticity of the Evidence," vol. 5075, Springer-Verlag Berlin Heidelberg, 2008, pp. 278-287.

[11] H. He, J. Zhang and H.-M. Tai, "A Wavelet-Based Fragile Watermarking Scheme for Secure Image Authentication," vol. 4283, Springer-Verlag Berlin Heidelberg, 2006, pp. 422-432.

[12] S.-C. Byun, S.-K. Lee, A. H. Tewfik and B.-H. Ahn, "A SVD-Based Fragile Watermarking Scheme for Image Authentication," vol. 2613, Springer-Verlag Berlin Heidelberg, 2003, pp. 170-178.

[13] G.-J. Lee, E.-J. Yoon and K.-Y. Yoo, "A New LSB Based Digital Watermarking Scheme with Random Mapping Function," in Ubiquitous Multimedia Computing, 2008.33,IEEE computer society, 2008.

[14] S. Fazli and G. Khodaverdi, "Trade-Off between Imperceptibility and Robustness of LSB Watermarking Using SSIM Quality Metrics," in ICMV '09 ,Second International Conference on Machine Vision, 2009.

[15] D. Basu, A. Sinharay and S. Barat, "Bit Plane Index Based Fragile Watermarking Scheme for Authenticating Color Image," in First International Conference on Integrated Intelligent Computing (ICIIC), 2010 , 2010.