International Journal on Recent and Innovation Trends in Computing and Communication
Volume: 2 Issue: 9

ISSN: 2321-8169
2908 – 2913

A Novel Approch for Digital Image Watermarking Using Cryptography

Nirdesh Jain
Research Scholar
Electronics and Communication Deptt.
SRIT
Jabalpur(M.P.), India
nirdesh_jain@yahoo.co.in

Rashika Gupta
Assistant Professor
Electronics and Communication Deptt.
SRIT
Jabalpur(M.P.), India

Abstract **-** Medicinal images can be made more secure by using enhanced watermarking technique; it allows us to embed the related information with the image, which provides secrecy, integrity and validation by embedding encrypted digital signature with the image. The diverse characteristics of watermarking algorithms are discussed in this paper. The performance evaluation of embedding the watermark in DWT domains is analyzed taking PSNR and MSE as the evaluation parameters. In this paper, data hiding and cryptographic techniques are combined into one secure simple algorithm. So, the original image is not mandatory at the time of watermark recovery. Because we insert final watermark in DWT domain, so this procedure is robust against many attacks.

Keywords: *Watermark, DWT, Encryption, Security, Medical Image, XOR transform*

*****

I. INTRODUCTION

Presently, most of the medical equipments are working in a computer network environment. Medical images are formed and stored in a digital form. It is well known that medical digital images can be malformed or manipulated with easiness. Furthermore, it is generally impossible to tell whether a given image is authentic or has been altered subsequent to capture by some readily available digital image processing tools. This is an important issue in medical archiving, where the medical image in question truly reflects what the scene looked like at the time of capture.

In the security domain, dependability service is explicitly defined as one, which guarantees that the sent and received data are alike. This binary definition is also relevant to images. In actual situations, images can be transformed; their pixel values can be modified but not the actual meaning of the image [1]. Security and competence of watermark data are very important issues to be considered. Watermarking is a rising research area for copyright protection and authentication of electronic documents and media. Most of the research is going on in this field, spatially in the field of image watermarking. The reason might be that there are so many images available at Internet without any cost, which needs to be protected [2].

A. Information Hiding

Digital Information hiding means communication of information by hiding in and retrieving from any digital media. The digital media can be an audio, an image, a video or simply a plain text file. However, generally Information hiding encompasses three disciplines: cryptography, watermarking, and steganography [3]. It is graphically shown in figure 1.1. Watermarking can be robust or fragile depending upon the application domain.

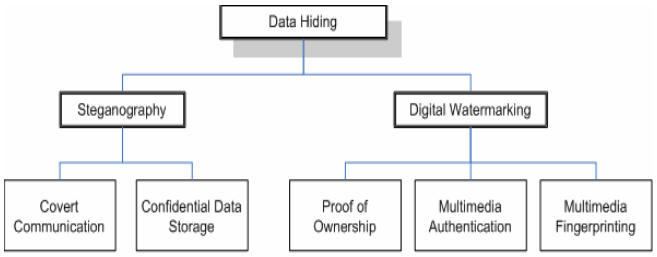

Figure 1.1 Classifications of Information Hiding Techniques

II. DIGITAL WATERMARKING

Watermarking is not a new technique. It is a descendent of a technique known as steganography. Steganography is a technique for secret communication. In distinguish to cryptography where the content of a communicated message is secret, in steganography the message is undisclosed and only parties involved in the communication know its presence. Steganography is a procedure where a covert message is hidden within another unrelated message and then communicated to the other party. Steganography is the science of communicating information while hiding the existence of the communication.

A. Necessity of Watermarking

In recent years it has been seen a rapid growth in network multimedia systems and other numerical technologies. This has led to an increasing awareness of how easy it is becoming to reproduce data. Because of the concern over copyright issues, a number of technologies are

being developed to protect against illegal copying. One of these technologies is the use of digital watermarks [4]. Digital watermarking allows an owner to safely post an image for viewing but legally provides an embedded copyright to prohibit others from posting the same image. So for security and robustness the data digital watermarking is necessary.

B. Watermark properties

To be considered as a good watermark, each type of watermark must meet some requirements as agreed upon by Cox et al. in [9] and Dittmann in [10]. The following being the most important:

1) Robustness: A watermark message is called robust, if even after any modification on the watermarked data, it can be reliably detected. The modification being for example compression in images, amplification of audio data, format conversions like mp3, JPEG etc.

2) Imperceptibility: A watermark is called imperceptible if one is not able to hear or see the difference between the original and the watermarked content. A watermark message hence shall not generate an audible or visual difference that can be noticed by hearing or vision.

3) Security: A watermark message is called secure, if the watermark message cannot be destroyed or detected, in case the data has undergone some attacks. Even if the watermarking algorithm is known to the attackers and they possess at least one watermarked copy, the watermark message must not be detected as the attackers do not know the secret key. In other words, the security of the watermark message must only depend on secret key possessed by the distributor alike typical cryptographic models.

***4) Capacity*:** It should be possible to embed a watermark message multiple times in one multimedia. How much information can be embedded into the original data is referred to as capacity. It is recommended to embed a message several times to increase the reliability of the detection process.

III. FRAMEWORK FOR WATERMARKING

The digital watermarking system essentially consists of a watermark embedder and a watermark detector (Figure 2.1). Digital watermarking is a technique to imperceptibly hide information, also called watermark message in multimedia data [3]. A Watermarking algorithm consists of two stages, the embedding stage and the detection stage. In the embedding stage, the watermark is integrated into the multimedia data using a secret key. The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e. prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks [5].

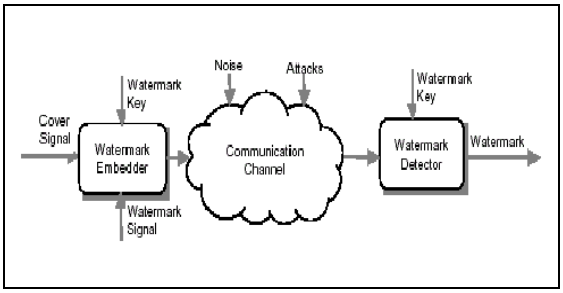

Figure 3.1 General Watermarking Systems

IV. TYPES OF DIGITAL WATERMARK

Watermarks and watermarking procedure can be divided into various categories in various ways. Watermarking method can be divided into four categories according to the type of file to be watermarked as follows [6]:

i. Video Watermarking
ii. Image Watermarking
iii. Audio Watermarking
iv. Text Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

i. Invisible-Robust watermark
ii. Visible watermark
iii. Invisible-Fragile watermark

V. ATTACKS

Watermarking method should be interfering resistant to hostile attacks. Depending on the purpose, the watermarked content encounters definite types of attacks. Some types of attacks are more significant than others [7]. Some basic types of attack are:

A. Active attacks

In this type of attack the hacker tries to eliminate the watermark or make it undetectable. This type of attack is crucial for many applications, including owner identification, fingerprinting, proof of ownership and copy control, in which the reason of the mark is overcome when it cannot be detected. However, it is not a serious crisis for verification or hidden communication.

B. Passive attacks

In this case, the hacker is not proposed to remove the watermark, but to notice its existence or existence of a covert communication. In most of the above reveal application areas, we are not worried by this type of attack. In fact, we mainly use visible watermarks making it

ISSN: 2321-8169
2908 – 2913

apparent that a watermark exists. But for hidden communication, the main concern is to hide the existence of a watermark.

C. Collusion attacks

These are a unique case of active attacks, in which the hacker uses a number of copies of one piece of media, each with a diverse watermark, to build a copy with no watermark. Opposition to collusion attacks can be critical in a fingerprinting application, which involves putting a different mark in each copy of a portion of media. However, the number of copies that we can expect the hacker to accomplish varies greatly from application to application. A collusion attack would involve that several employees scheme to take the matter, which is an unlikely prospect.

D. Forgery attacks

In this attack, the attacker tries to integrate a legitimate watermark, rather than removing one. These are our main security disquiet in authentication applications, because if hackers can push in valid verification marks, they can cause the watermark detector to accept forged or customized media. This type of attack is a serious concern in proof of ownership.

VI. PROPOSED WATERMARK EMBEDDING AND EXTRACTION METHODOLOGY

The various steps for embedding and extracting the watermark in DWT domain are given below.

A. Watermark Embedding Algorithm Input

1. Read the CT image (cover image).
2. Read the signature (watermark).
3. Fix the alpha value to 1 (alpha=1).
4. Multiply the alpha value with the sign.
5. Take the transform for the image (DWT).
6. Watermark 1 – a binary image act as a watermark that embed in the main watermark.
7. Watermark 2 – a binary image act as main watermark.
8. Cover Image – gray scale image to be watermarked.
9. E1 – key used for encrypting Watermark1.
10. E2 – key used to encrypt watermarked watermark.
11. W1 – key used to embed encrypted binary watermark into the main watermark.
12. W2 – key used to embed encrypted watermarked watermark in Cover Image.
13. Calculate the MSE and PSNR between the original and watermarked image.
14. Increment the alpha value and repeat the steps from 4 to 14.

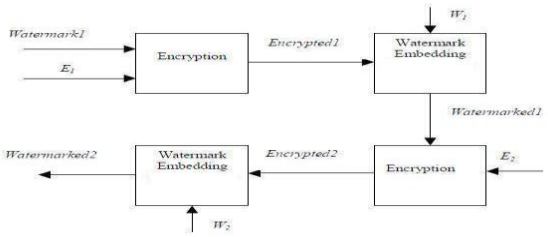

Figure 6.1 Block Diagram of Watermarks Embedding Procedure Algorithm

Algorithm

1. Take Watermark1 and encrypt it by performing XOR operation with the key E1. This output is called Encrypted1.
2. Apply procedure to insert Encrypted1 in the second binary watermark image (Watermark2) using key W1. This output image is Watermarked1.
3. Again encrypt Watermarked1 using XOR with key E2 to give the output image Encrypted2.
4. Apply procedure embed Encrypted2 in the gray-scale Cover Image using key W2. This Output image is the final watermarked image and called Watermarked 2.

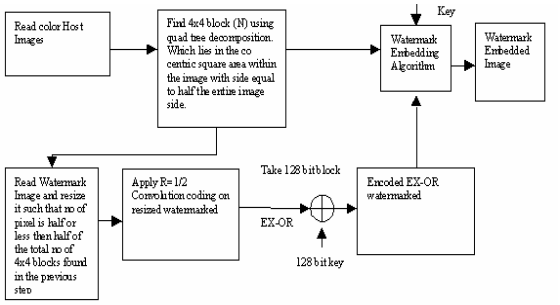

Figure 6.2 Watermark Insertions with XOR Operation

Output

Watermarked2 – finally watermarked image

B. Watermarks Extraction Algorithm

Input

1. Watermarked2 – it is the received watermarked image.
2. Take the transform for the image (DWT).
3. Read the signature
4. Divide the signature by the alpha value
5. Subtract the signature from the watermarked image
6. Take the inverse transform
7. S1 – size of watermark1.
8. S2 – size of watermark2.
9. E2 – key used to decrypt Recovered watermark from cover Image.
10. E1 – key used for decrypting Recovered Watermark from main watermark.
11. W2 – key used to recover encrypted watermarked watermark from Cover Image.

 ISSN: 2321-8169
2908 – 2913

12. W1 – key used to recover encrypted binary watermark from the main watermark.
13. Reconstructed image is obtained
14. Calculate the PSNR and MSE of the original and recovered image and the original and retrieved watermark.

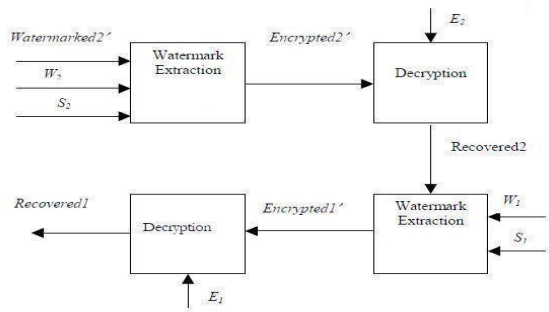

Figure 6.3 Block Diagram of Watermarks Extraction Procedure Algorithm

Algorithm

1. Apply method to extract encrypted watermark2 from Watermarked2 using key W2. The improved and recovered image is Encrypted2'.
2. Decrypt Encrypted2 using XOR with key E2. The output of this step is called Recovered2.
3. Apply method to extract encrypted watermark1 from Recovered2 using key W1. This recovered image is called Encrypted1'.
4. Decrypt Encrypted1 using XOR with key E1. The output of this step is called Recovered1.

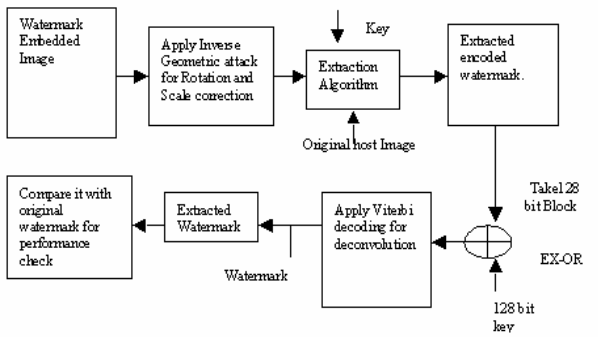

Figure 6.4 Watermark Extractions with XOR Operation

Output

Recovered2 – main watermark recovered from the received watermarked image.

Recovered1 – watermark recovered from the main watermark.

VII. EXPERIMENTAL RESULTS

In our experimental results three images are used as cover images. We measure the quality of watermarked images in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). In best case PSNR should be infinite and MSE should be zero. But it is not feasible for all watermarked image. So, large PSNR value and small MSE value is desirable. To verify that if the recovered watermark is the same to the one that is embedded, we calculate only MSE. In our case it should be zero. We see the effect of embedding nested watermark in each image. Summary of these results is shown in the table 7.1. Figures 7.1, 7.2 and 7.3 show the watermarking of all images in detail.

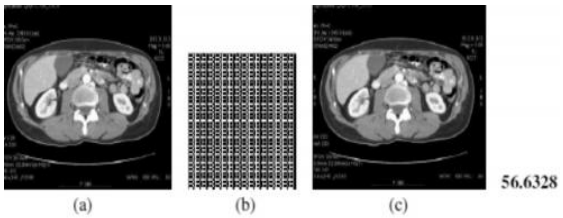

Figure 7.1 (a) Original Image, (b) Watermark Image, (c) Watermarked Image with PSNR (dB) Value

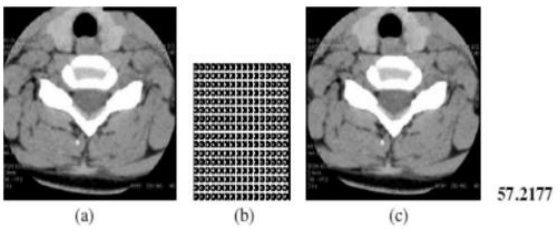

Figure 7.2 (a) Original Image, (b) Watermark Image, (c) Watermarked Image with PSNR (dB) Value

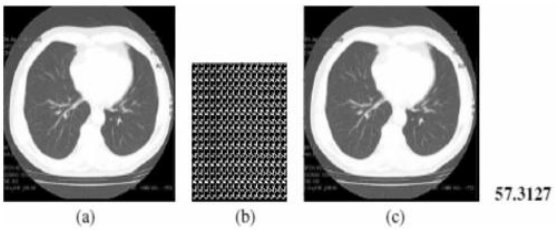

Figure 7.3 (a) Original Image, (b) Watermark Image, (c) Watermarked Image with PSNR (dB) Value

Summary of PSNR and MSE for watermark insertion and extraction results-

PSNR1 – PSNR of main watermark after embedding watermark1 in it

PSNR2 – PSNR of gray scale cover image after embedding watermarked watermark

MSE – MSE of main watermark after embedding watermark1 in it.

Cover Image	Water-mark 1	Water-mark 2	PSNR1 (dB)	PSNR2 (dB)	MSE
Image 7.1(a) Original Image	Image7.1(b) Watermark Image	Image 7.1 (c) Watermark Image	24.264	56.632	0.018
Image 7.2(a) Original Image	Image7.2(b) Watermark Image	Image 7.2 (c) Watermark Image	25.184	57.217	0.019
Image 7.3(a) Original Image	Image7.3 b) Watermark Image	Image 7.3 (c) Watermark Image	25.273	57.312	0.028

Table 7.1 Watermark Insertion and Extraction Results

VIII. PERFORMANCE EVALUATION PARAMETERS

To evaluate of the watermarking algorithm, different criteria's are used. Some of the significant among them are the quality, security and the robustness of the watermarking scheme against various attacks. Among the most important distorting measures in image processing is the Signal to Noise Ratio (SNR) and the Peak Signal to Noise Ratio (PSNR). The SNR and the PSNR are respectively defined by the following formulas:

$$PSNR = 10\log_{10}\left(\frac{MAX}{MSE}\right)$$

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(X(m,n) \quad X_w(m,n))^2$$

in units of dB, where X is host signal, w is the watermark X w is the watermarked signal MN , is the total number of pixels in X or X w, MAX is the maximum pixel value in the image.

The first experiment is conducted to select the domain of watermarking. The watermark is first applied in the DWT domain and the performance is evaluated based on PSNR and MSE. So, the next step aims to find out which wavelet transform that can be used for the embedding purpose and also to find out the level of decomposition, for that three sets of mother wavelets are considered "Haar", "db2" and "db4". The result shows that Haar gives better performance compared to the others.

IX. SECURITY INCREASE RESULTS

In our watermarking method we used encryption. So, in any case if watermarking key is disclose and attacker extracts the watermark, still the attacker will not be able to read the watermark because it is still encrypted. In our watermarking method user need four keys for watermark extraction. If any of keys is invalid, then user will not be able to extract both watermarks correctly. Either one or both the watermarks will be incorrect. It depends upon which key is invalid. This concept is shown in the given table-

Key E1	Key E2	Key W1	Key W2	Recovered Watermark2	Recovered Watermark 1
Valid	Valid	Valid	Valid	Recovered	Recovered
Invalid	Valid	Valid	Valid	Recovered	Not Recovered
Valid	Invalid	Valid	Valid	Not Recovered	Not Recovered
Valid	Valid	Invalid	Valid	Recovered	Not Recovered
Valid	Valid	Valid	Invalid	Not Recovered	Not Recovered
Invalid	Invalid	Invalid	Invalid	Not Recovered	Not Recovered

Table 9.1 Key Based Security Results

X. CONCLUSIONS

In this paper, an effective watermarking scheme is presented for the integrity and authenticity verification of medical images. The diverse characteristics of watermarking algorithms are discussed in this paper. The performance evaluation of embedding the watermark in DWT domains is analyzed taking PSNR and MSE as the evaluation parameters. In this paper, data hiding and cryptographic techniques are combined into one secure simple algorithm. It consists of image encryption, embedding, extraction and then decryption or recovery of the original image. Before embedding we encrypted both the watermarks with XOR operation. This provides an additional level of security for watermarks. If watermarking key is hacked still the attacker will not be able to identify the watermark because it is encrypted. The encryption/decryption is only achieved using keys generated ahead of both operations for that purpose. The method described in this paper is more secure. The future work has to be extended by evaluating the robustness of the watermarking algorithm against different types of attacks such as geometric attacks, compression attacks and modify further. Future enhancement to the current method would be to use more secure cryptography with advanced key designs to hide sensitive images.

REFERENCES

[1] Memon N. Watermarking of medical images for content authentication and copyright protection. PhD thesis, Pakistan: Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology; May 2010.

[2] Robert, L., and T. Shanmugapriya, "A Study on Digital Watermarking Techniques ", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

[3] F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn, "Information hiding - A survey", Proceedings of the IEEE, vol. 87, no. 7, 1999, pp.1062– 1077.

[4] Dr. Martin Kutter and Dr. Frederic Jordan, "Digital Watermarking Technology", in AlpVision, Switzerland, pp 1 – 4.

[5] Lu, C. S., Huang, S.-K., Sze, C.-J., Liao, H.-Y., "A new watermarking technique for multimedia protection'', in Multimedia Image and Video Processing, L. Guan, S.-Y. Kung, and J. Larsen, Eds. Boca cRaton, FL: CRC, pp. 507 –530, 2001.

[6] Robert, L., and T. Shanmugapriya, "A Study on Digital Watermarking Techniques ", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

[7] D. Boneh and J. Shaw. Collusion-secure _ngerprinting for digital data. IEEE Transactions on Information Theory, 44(5):1897{1905, Sept. 1998.

[8] ZuneraJalil, M. ArfanJaffar, and Anwar M. Mirza, "A Novel Text Watermarking Algorithm Using Image Watermark", International Journal of Innovative Computing, Information and Control (IJICIC) (indexed by ISI with Impact Factor 2.93) (Scheduled to be published in February, 2011)

[9] I. J. Cox, M. L. Miller, and J. A. Bloom. Digital Watermarking. Morgan Kaufmann, 2002.

[10] J. Dittmann and M. Steinebach. Joint watermarking of audio-visual data. In Proc. IEEE Fourth Workshop on Multimedia Signal Processing, pages 601{606, 3{5 Oct. 2001}}.

[11] Remya Elizabeth Philip, Sumithra M.G. / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 1, January -February 2013, pp.962-968

[12] B. M. Plantiz, A. J. Maeder, "A Study of Block-Based Medical Image Watermarking Using a Perceptual Similarity Metric", Proceedings of the Digital Imaging Computing: Techniques and Applications (DICTA 2005), 2005.

[13] R. Raul et al., "Hiding scheme for medical images", Proc.17th International Conference on Electronics, Communications and Computers, ,pp. 32-32 August 2007.

[14] Mohamed Ali Hajjaji, Abdellatif, El-bey,"A watermarking of Medical Image: Method Based LSB", Journal of Emerging Trends in Computing and Information Sciences, Vol.2, NO.12, December 2011.

[15] J. Bernarding, A. Thiel, and A. Grzesik. A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encrytion. International Journal of Medical Informatics, 64:429–438, 2001.

[16] R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl. Confidential storage and transmission of medical image data. Computers in Biology and Medicine, 33:277–292, 2003.

[17] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012 ISSN 2229-5518.