International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No. - 8, Issue No. - 5, September, 2020

Study of Digital Image Security using Cryptography and Data Hiding

Koppula Manasa
Electronics & Communication Engineering
Balaji Institute of Technology & Sciences
Warangal, India
E-mail: manasa436@gmail.com

Bandi Mounika
Electronics & Communication Engineering
Balaji Institute of Technology & Sciences
Warangal, India
E-mail: gmounika0509@gmail.com

Abstract— The implementation of a system that combines encoding standards with watermarking techniques to produce security to changed medical images is that the main concern of this paper. The system is based on a hybrid algorithmic rule that applies the techniques of encoding and watermarking to supply completely different security features to medical pictures transmitted between attention entities. Supported the planned algorithm, the genuineness and integrity of the transmitted pictures square measure typically verified either inside the special domain or inside the encrypted domain or in each domain. This is achieved by connection the watermarked image and its encrypted version once embedding 2 distinctive watermarks; one inside the plain image and one inside the encrypted image. The planned algorithmic rule makes use of the idea of bit planes wherever 2 pictures consists of 8- bit planes combined to form one image having 16-bit planes. The algorithmic rule provides high embedding capability while keeping low procedure complexness.

Keywords-Medical images; digital watermarking; cryptography; bit planes

I. INTRODUCTION

The continuous and important advancements in information and communication technologies expedited sharing of digital medical pictures in telemedicine applications. However, thanks to the sensitive and important nature of medical pictures, their security has become a challenging demand that has got to be addressed. To provide safe transmission of medical pictures between completely different health entities, science techniques and digital watermarking technologies are wide used.

In cryptography, encoding standards and digital signatures square measure wont to give confidentiality, genuineness, and integrity to changed pictures [5,7]. However, the medical pictures square measure subject to completely different types of manipulations and outlaw distribution once they get decrypted at the receiving health entity. On the opposite hand, digital watermarking techniques are planned in recent years for embedding data into objects such as images, audio signals, and video frames, which may be used for media notation, copyright protection, integrity authentication, and covert communication [1,3]. Therefore, digital watermarking technologies can do authenticity and integrity by embedding management information watermarks within the digital objects, whereas confidentiality isn't achieved. to match the 2 technologies, encoding is taken into account a pre protection mechanism, whereas digital watermarking will thought-about as a posteriori management mechanism as a result of the image content remains available for interpretation whereas the remaining is protected [8].

In this paper a information concealment algorithmic rule supported watermarking and encoding techniques is planned. The algorithm makes use of the idea of bit planes wherever it combines 2 pictures every consisting of 8-bit planes throughout a single image consisting of 16-bit planes. The algorithmic rule will be seen as using partial encoding of the two joined 8- bit plane pictures since the combined image has the encrypted and plain bit planes shuffled. On the opposite hand, it can be seen as using full encoding at the receiver aspect wherever the two pictures square measure separated and processed. The algorithmic rule has distinctive options that makes it effective for secured transmission of medical pictures.

One feature is that it increases the embedding capability by an element of 2 since two copies of the cover image square measure used for knowledge embedding. In every copy of the image, a singular watermark is embedded and accessed by a special key. Another distinctive feature of the algorithmic rule is that it decreases the aspect data that must be sent to the receiver by concatenating it with the watermark payload, therefore increasing the quantity of information embedded within the image. This can be done by feeding the aspect information to a key generator to provide 2 concealment keys for concealment knowledge inside the spacial and encrypted domains.

The overall performance of the planned algorithmic rule could be a trade-off between completely different performance metrics. These metrics embrace the whole embedding capability offered by the spatial and encrypted domains, the watermarked encrypted image entropy, and also the physical property of the directly decrypted image. intensive experimentations are conducted to guage the performance of the algorithmic rule. The achieved performance results demonstrate that the planned algorithm square measure typically applied effectively to medical pictures since it provides security to the changed pictures whereas reassuring their actual recovery at the receiver's aspect. The reminder of this paper is organized as follows. Detailed description of the planned algorithmic rule is given in section 2. The performance results of the algorithmic rule square measure presented in section 3. Finally, last remarks square measure outlined in section four.

II. THE PROPOSED ALGORITHM

This proposed algorithm makes use of the construct of bit planes. It combines 2 pictures every consisting of 8-bit planes

in an exceedingly single image consisting of 16-bit planes. The algorithm are often seen as using partial secret writing of the two joined 8-bit plane pictures since the combined image has the encrypted and plain bit-planes shuffled. On the opposite hand, it are often seen as using full secret writing at the receiver facet wherever the 2 pictures ar separated and processed.

A. Watermarks Embedding Procedure

The secret writing employed in this technique is pel permutation. The operational steps of the watermarks embedding procedure is delineated below and its diagram is shown in Figure1.

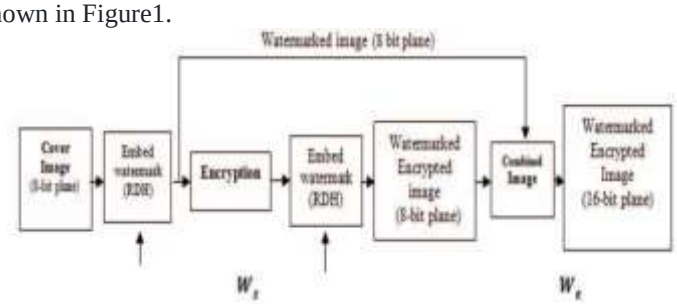

Figure1. diagram of the watermarks embedding procedure of the projected algorithmic program.

Step1: infix the spacial domain watermark Ws within the image mistreatment bar graph Shifting RDH technique. Save a version of this watermarked image.

Step2: inscribe this watermarked image mistreatment pel permutation.

Step3: infix the encrypted domain watermark we tend to in the encrypted image mistreatment the RDH bar graph Shifting method.

Step4: mix the 2 images; the watermarked image and therefore the encrypted watermarked image every having 8- bit planes. This method creates a brand new image consisting of 16-bit planes in keeping with a pre-defined assignment of the bit-planes of those 2 pictures. The assignment makes positive that the encrypted image bit planes ar a lot of seemingly to be placed within the higher bit planes. as an example the bit plane assignment employed in the instance within the projected algorithmic program is shown in Table1.

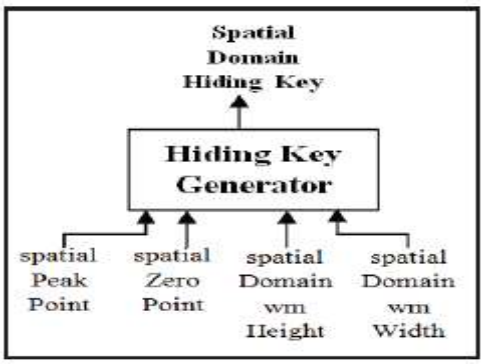

Figure 2. spacial domain-hiding key generator.

A unique feature of this algorithmic program is that it decreases the Histogram Shifting facet info by concatenating it with the payload, so increasing the pure embedding capacity. This can be done by feeding the facet info to a key generator to provide the info activity key. Figure2 shows the info things that ar accustomed generate the spacial domain-hiding key.

Table1. An Example Of Bit Plane Assignment Within The Combined Image

Combined image bit plane range	The corresponding Bit plane assignment
16	Encrypted image bit plane seven
15	Encrypted image bit plane eight
14	Encrypted image bit plane six
13	Encrypted image bit plane one
12	Encrypted image bit plane five
11	Encrypted image bit plane six
10	Encrypted image bit plane five
9	Encrypted image bit plane eight
8	Encrypted image bit plane four
7	Encrypted image bit plane four
6	Encrypted image bit plane three
5	Encrypted image bit plane three
4	Encrypted image bit plane two
3	Encrypted image bit plane two
2	Encrypted image bit plane seven
1	Encrypted image bit plane one

B. Watermarks Extraction Procedure

The extraction procedure is that the precise inverse of the embedding procedure. consequently, the watermarked encrypted watermarked image is split into 2 pictures using identical predefined bit-plane placement employed in the embedding procedure. Then every image is treated differently as delineated below. A diagram of the watermarks extraction procedure is shown in Figure3.

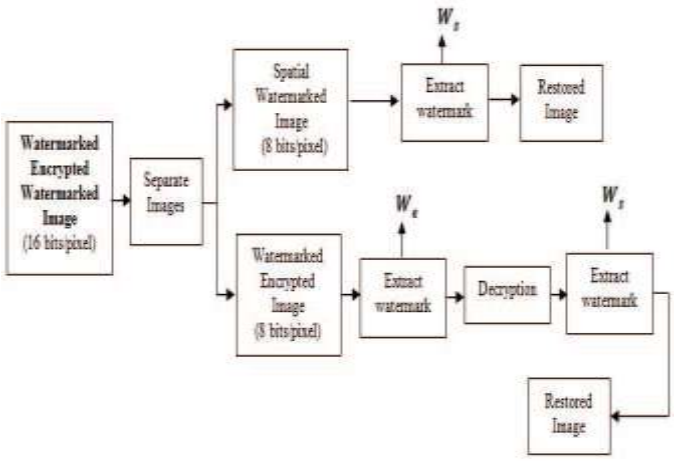

Figure3. diagram of the watermarks extraction procedure within the proposed algorithm.

Step1: mistreatment the pre-defined bit plane assignment, which was employed in the embedding procedure, recover the bit planes of the watermarked and encrypted pictures and reconstruct them.
Step2: If the spacial domain activity key's offered, take the watermarked image and extract the spacial domain watermark. This produces an explicit restored version of the image.
Step3: If the secret writing domain activity key's offered, take the encrypted image, extract the encrypted domain watermark, and so decode the image.
Step4: To revive the precise image from the encrypted part, the spacial domain embedded watermark should be extracted from this decrypted image.
Step5: Reconstruct the 2 domains watermarks, and two copies of the first 8-bit image.

III. PERFORMANCE RESULTS

In this section we tend to gift the performance results of the proposed algorithmic program. Medical pictures of 4 modalities (CT, MRI, UltraSound, X-RAY) are used for analysis. Three metrics were accustomed assess the performance, maximum embedded capability, visual quality, and entropy of the watermarked image. The performance results rumored in this section ar for the spacial domain, the encrypted domain, and therefore the 2 domains combined along.

A. Performance of the Spacial Domain

The performance of the projected algorithmic program within the spatial domain is evaluated by mensuration 2 parameters: the maximum offered embedding capability measured by bits per pel (bpp) price, and therefore the quantity of distortion introduced to the first image when inserting the spacial domain watermark measured by the height signal to noise ratio (PSNR). The results ar summarized in Table2.

Table2. Spacial Domain Results For Various Medical Modalities

Test Image	PSNR(db)	Embedded Watermark Size (bits)	Max bpp
CT	56.792	90,000	0.4800
MRI	64.219	90,000	0.0674
US	54.880	90,000	0.1763
X-RAY	66.726	90,000	0.0327

In As are often noticed in Table2, there's a exchange between the physical property of the spacial watermarked image measured by PSNR and therefore the embedding magnitude relation measured by bpp. This exchange is apparent within the X-RAY image results since it achieved the most effective PSNR magnitude relation however the least embedding capability bpp. The CT pictures achieved the best performance in terms of the embedding capability whereas maintaining terribly acceptable PSNR values.

B. Performance of the Encrypted Domain

The performance of the projected algorithmic program within the encrypted domain is measured with the utmost offered embedding capability additionally to the entropy price of the 8-bit encrypted image. The results ar summarized in Table3.

Table3. Encrypted Domain Results For Various Medical Modalities

Test Image	PSNR(db)	Max bpp	Image Entropy
CT	56.653	0.4511	4.6552
MRI	63.979	0.0508	6.4717
US	54.780	0.1475	7.0058
X-RAY	64.529	0.0275	7.2498

Table3 shows a comparison between the encrypted and the 'watermarked encrypted' 8-bit pictures with respect to the achieved PSNR magnitude relation and also the most accessible embedding capability. The trade-off exists between the imperceptibility and capability, kind of like the spacial domain case that was delineate higher than. The X-RAY pictures achieved the most effective PSNR ratios whereas the CT pictures achieved the utmost bpp values. The entropy values of the encrypted 8-bit pictures of various modalities aren't very high normally. The smallest amount entropy worth was recorded for the CT pictures and also the highest worth was recorded for the X-RAY pictures.

C. The Overall Performance

The performance of the combined image within the projected algorithm is measured with regard to the utmost available embedding capability that the 2 domains will provide and also the entropy values of the ultimate encrypted watermarked image. A comparison between the results achieved for the various take a look at pictures is given in Table4.

Table4. Combined Encrypted Watermarked Image Results For Various Medical Modalities

Test Image	Watermarked Encrypted Image Entropy	Max bpp
CT	5.3894	0.9312
MRI	6.2289	0.1183
US	7.6468	0.3239
X-RAY	7.7072	0.0602

As will be noted in Table IV, the entire embedding capacity of the 16-bit image is that add of the embedding capacity of the spacial 8-bit image and also the embedding capacity of the encrypted 8-bit image. Another notice is that the X-RAY image achieved the very best entropy worth, which shows that there exists a trade-off between the image maximum accessible embedding capability and its entropy value. this could even be seen for the CT 16-bit image which achieved a complete embedding capability of (0.93) bpp but a coffee entropy worth of (5.39).

IV. CONCLUSION

In this paper a crypto watermarking algorithmic program has been proposed to attain high embedding capability in medical images. This has been achieved by connexion the watermarked image and its encrypted version, when embedding 2 different watermarks within the combined image. The algorithm makes use of the construct of bit planes that allows connexion 2 pictures, every consisting of eight bit-planes, in a single image having sixteen bit-planes. The

novelty of the proposed algorithmic program is in its ability to use reversible information hiding and coding techniques to the total image by producing 2 copies of the image which will be treated differently. connection 2 copies of the image, a spatial domain copy associated an encrypted domain copy, results in doubling the embedding capability. Another feature of the algorithm is that it provides image security at totally different stages and guarantees blind watermark extraction. Experiments were performed exploitation four medical modalities: CT, MRI, Ultrasound, and X-RAY. The results demonstrate that the algorithmic program will be applied effectively to medical images of various modalities since it offers a certain cowl image changeability while not errors within the extraction part.

REFERENCES

[1] X. Guo, T. Zhuang, "A region-based lossless watermarking scheme for enhancing security of medical data," Journal of Digital Imaging 22(1): (2009) 53-64.

[2] W. Stallings, Cryptography and Network Security—Principles and Practice. E NJ: Prentice-Hall, 2016.

[3] Ali Al-Haj, Ahmad Mohammad , and Alaa Amer "Crypto-Watermarking of Transmitted Medical Images", Journal of Digital Imaging, pp. 1-15, August 2016. DOI 10.1007/s10278-016-9901-1

[4] C. Tan, C. Ng, X. Xu, C. Poh, L. Yong, and K. Sheah, "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," Journal of Digital Imaging, 24(3), (2011) 528–540.

[5] Ali Al-Haj, Gheith Abandah, and Noor Hussein, "Crypto-based algorithms for secured medical image transmission", IET Information Security, 9(6), pp. 365-373, Nov. 2015.

[6] Hong et al. ,"An improved reversible data hiding in encrypted images using side match," IEEE Sig. Proc. Lett., 19(4) (2012) 199-202.

[7] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. For. Security, 7(2), (2012) 826-832.

[8] Ali Al-Haj (Editor) *Advanced Techniques in Multimedia* Watermarking*: Image, Video and Audio Applications*, IGI Global, USA, April 2010.

[9] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, (2011) 255-258.

[10] Ali Al-Haj, Noor Hussein, and Gheith Abandah "Combining Cryptography and digital watermarking for secured transmission of medical images," in Proc. of the IEEE Int. Conf. Inf. Management, UK, May 2016.