Medical Image Watermarking Based on Secret Sharing and Integer Wavelet Transform

Gaidaa S Mahdi¹, Noor A Yousif² and Abeer F Shimal³

¹ Chemical Eng. Dept., University of technology-Iraq, Bagdad, Iraq
²,³ Control and Systems Eng. Dept., University of technology-Iraq, Bagdad, Iraq
Email: gaidaa.s.mahdi@uotechnology.edu.iq, 60028@uotechnology.edu.iq and Abeer.F.Shimal@uotechnology.edu.iq

Abstract
In telemedicine, the medical data are shared and distributed between the whole world with different specialists and for many purposes through an unsafe medium. So protecting the medical data during the transmissions becomes an important issue. Many image secret sharing schemes with steganography have been proposed. Unfortunately, each of these schemes has one or more drawbacks. First, the large size of a stego images. Second, the visual quality of the stego images evaluated by the peak signal-to-noise ratio (PSNR) is degraded too much. To overcome such drawbacks, a new scheme based on secret sharing and IWT is proposed in this paper. The new scheme can optimize both the size of the stego images and its quality. The proposal scheme involves a dispersion of medical image into shadow images using Lin and Thien’s technique. The size of each shadow size is reduces to \(1/k\) from the overall of the secret image size and \(k\) is the number of shadows. After that, the shadows are embedded in a host image by using Integer wavelet transform (IWT) technique. In the reconstruction the secret medical image is reconstructed by pooling at least \(k\) shadows. The experimental results of the proposed algorithm are shown for many medical images the effectiveness of analyzed with the help of the peak signal-to-noise ratio and normalized correlation.

Keyword: Secret sharing, Watermarking, IWT, Medical image, Thien and Lin’s technique.

1. Introduction
A huge area of storage and recovery data can be obtained by saving text files and medical image in a computer. A database of full information for each patient is obtainable in one place rather than a dispersed system. Many applications like teleconsultation and telemedicine require data and information transfer over an unsafe network. The safety of confidentiality and integrity of the patient’s information and his medical image is a security matter. During the transmission through unsecure channel the medical image must not be altered. Besides above, the medical records and images can be used as an educational element in the medical area, evidence in legal trials and insurance demands. The Security of medical information and images enriched with confidentiality, authentication and integrity has become a big area for research [1, 2].
In medical, commercial and military systems the secure protection and effective of secret images are the main goal. The confidential images must be encrypted from being illegally accessed. However, a common problem is that these encrypted images are maintained in a single information-carrier. For example, the secret image cannot be reclaimed if the encrypted image is missing or corrupted over the transmission. To deal with this security issue, a process of secret image sharing had been introduced. The secret image is shared between a group of candidate or participants. The certified subgroups of the participants can collaborate to reconstruct or restore the genuine secret image; unqualified subgroups will not have any information about it [3].

The first conception of the (k, n) was presented by Shamir using secret sharing scheme of threshold [4]. The secret data is hidden in the fixed (constant) term of a (k−1)-degree polynomial to generate n shadows (known as shares), where every k (k ≤ n) or many more shadows will be collected to reconstruct and restore the secret data, while each k − 1 or less shadows can have no information about it (secret data). An important category of secret image sharing is the visual cryptography scheme (VCS) proposed by Shamir and Naor [5]. Another category of sharing scheme for image secret is design using the polynomial. In 2002 Lin and Thien proposed a (k, n)-threshold polynomial-based image secret sharing scheme [6]. They hide the pixels (secret) in every coefficients of a (k − 1)-degree polynomial to divide every secret image into n noise-like shares, also called shadow images. The size of each shadow image is only 1/k of that of the secret image. Many polynomial-based image secret sharing schemes were proposed for smaller size of shadow images [7, 8].

Since each shadow image is noise-like, it may attract the attention of attackers and is not convenient for management. A few data hiding approaches can be used to hide the shadow images in some ordinary images. Wu et al. proposed a secret image sharing and hiding approach without size expansion [9]. A pre-processing quantization procedure is developed for compressing the secret image. Then the compressed secret image is used to generate shadow images based on polynomial, finally the shadow images are hidden in the cover images. However, the generated image with the shadow image embedded in, called stego image, has noticeable deterioration of visual quality. Furthermore, their scheme is lossy for secret image, which is not applicable for situations like military, medical and fine art image keeping and preservation. Some researchers employed the modulus operator to reconstruct the distortion-free cover image [10, 11]. An enhanced scheme based on PSNR estimation is proposed by [3]. At first the secret image shared into a shadow images by polynomial-based secret sharing scheme. Then, every shadow image is hidden in a cover image by the proposed (s, c) hiding technique depending on the PSNR estimation.

In [12], proposed a safe sharing image scheme with high quality stego-images. In this method a preprocessing approach was used where the secret image is compressed so the statistical correlations among neighboring pixels of the secret image fall significantly, this result in enhancing the visual security of the proposed approach and reduced the size needed of the image cover. During the reconstruction of the secret image and in order to find three types of deception, the authentication code of the hash-based message of an image share, the identity ID of a participant and the value of argument x are embedded in the cover image with the image share, Beside that, the security of our scheme is better and enhanced because of the application of both dynamic embedding and random strategy. In [13] a useful SISS is introduced based on Natural Steganography (MSISS-NS). At first, by using the Chinese Reminder algorithm the secret image is divide into n small sized shadow images, then they are embedded into RAW images to simulate image using higher ISO parameters with NS. In MSISS-NS, the shadow images visual quality of has enhanced greatly. In addition to, each cover images payload together with the Ns which is larger in size comparing to the shadow images (small size), this scheme work very good not only in visual camouflage but also in many area such as recovery without losing data, no pixel expansion and steganalysis resisting. In [14] put forward a (2, n) progressive VSS with
successful (meaningful) shares. However, other researchers in [15] primarily concentrated on the medical image safety and security using the EVSS and the recovering and sharing process didn’t lose information and had few complications. The above two methods are bounded by the threshold.

2. **Proposed System**

The \((k, n)\) threshold Secret Image Sharing scheme (SISS) solved the image protection issue. However, the traditional SISS which used to generate noise-like shadow images that trigger suspicions easily, that’s why it’s important to generate strong shadow images. Many solutions found, one of them is to use a natural image (meaningful) and embed the shadow image in it considering the image visual quality. Limited by the embedding rate, the design scheme has made privileges in visual quality and size of the shadow images. The proposed method used a secret image sharing based on Thien and Lin’s technique and hiding technique based on IWT. The proposed method involves the dispersion of medical image into shadow images using Lin and Thien’s technique. Each shadow size is reduced to \(1/k\) from the total secret image size. Next, every shadow is embedded in the host image by using Integer wavelet transform (IWT) technique. Through the reconstruction, at minimum \(k\) shadows are pooled to reconstruct the medical secret image. Figure 1 shows the block diagram of the sharing model of proposed method.

![Figure 1: The proposed method showing the sharing model.](image-url)
The revealing process of a secret image is the reverse of the sharing process procedure. Calculating for the proposed scheme using threshold \((k, n)\), the secret image can be restored by any \(k\) of the meaningful shadow images. At first, a small-sized shadow images is recovered by \(k\) which are extracted from the host images. Then, the recovered secret image \(S'\) is rebuild from \(k\) shadows of the extracted shadows. Figure 2 depicts the recovery design for the proposed method.

![Any k of stego shadow images](image)

**Figure 2:** A design for the proposed method recovery.

### 2.1 Generate \(n\) Shares Based on Thien and Lin’s Technique

This method is applied for share generation. It a \((k, n)\) threshold-based image secret sharing scheme (SSS) by intelligently using Shamir’s SSS to create sharing images. Main idea is to use and benefit from the polynomial functions of the order \((k - 1)\) to build or construct \(n\) image shares created from an \(l \times l\) pixels of the secret image (named \(I\))

\[
S_x(i, j) = I(ik + 1, j) + \ldots + I(ik + k - 1, j)x^{k-1} \pmod{p}
\]  

where \(0 \leq i \leq \left\lfloor \frac{l}{k} \right\rfloor\) and \(1 \leq j \leq l\). This approach reduces image shares size to become \(1/k\) from secret image size. Any \(k\) image shares can rebuild the value of each pixel in the secret image. A few research insights made by Thien and Lin for image recovery without losing data by using their technique.

Figure 3 illustrated a representation of \((2, 4)\) secret image that share a construction process where \(n=4\) and \(k = 2\). As seen in this technique, a polynomial function of the first order can be formed as

\[
S_x(i, j) = (110 + 112x) \pmod{251}
\]  

![Shadow images extraction](image)

![Revealing phase](image)

![Restored secret image](image)
where 112 and 110 represent the first two pixel values in a brain image. However, the four participants, Four x values is being picked in a random way then substitute them in a polynomial function by giving \( p \) a value equal to 251 (the biggest prime number below 255) the maximum gray value of the image. Four shares is being computed which are (1, 222), (2, 83), (3, 195) and (4, 56). In the four image shares they become a number one pixel. The second pixel can be calculated in a similar way by constructing another group of a polynomial function of the first order using the following two pixels in the brain image. This procedure lasts until each pixel is encoded. Figure below shows the four shares image in the bottom right, the size of every image share equal to the half \((1/2)\) of main image size. Not any of the image shares shows seems to expose any information or data about the secret image. Anyhow, the pixels value of the natural image must not be random that’s because the value of the neighbor pixels are close or equal value. It is obvious that the values of the first two pixels (112 and 110) are extremely near to one another. This result in a probability of using single one of the secret share images to restore the secret image by presuming the value of the neighbor pixels is equal to the values in the polynomial function of the first order.

![Secret sharing process for brain Image.](image)

**Figure 3:** Secret sharing process for brain Image.

2.2 Hiding Shares in Meaningful Image

The domain transformation method offers the potential of embedding more information and stronger resistance to many common attacks. To avoid this downside of setting false confidence levels, an invertible wavelet transform based on lifting is used. Basically, it maps integers to integers with no loss of data across forwards and inverse. Each bit embedded in a block of \(2\times2\) from each meaningful host images. Then applied one level of IWT for each blocks to get four sub bands (LL, LH, HL, and HH) for each block. High frequencies may be lost by compression or scaling; therefore, the watermark will be embedded in the lower frequency by updating its value according to Equation (3). Besides, a quantization parameter \(Q_s\) can be used to achieve better performance in robustness. Herein we use LL sub-band to embed the signature. LL sub-band is first quantized by a scaling factor \(Q_s\), as in the following equation:

\[
q = \text{floor}\left(\frac{L_L}{Q_s}\right)
\]  

(3)

Where \(Q_s\) is a scaling factor.

Then embed bits of signature are as in Equation (4):
\[
LL = \begin{cases} 
(q \ast Q_s) + \left(\frac{Q_s}{2}\right) & \text{if } \mod(q, 2) = S(idx) \\
(q + 1) \ast Q_s + \left(\frac{Q_s}{2}\right) & \text{otherwise}
\end{cases}
\] (4)

For \(idx = 1\) to \(\text{length}(S)\)

After embedding the bit in \(LL\), apply the inverse of IWT on the current block. Algorithm 1 shows the steps of the embedding process.

**Algorithm 1: Embedding share**

| Input: |
|--------|
| HI // host image |
| S // The share |

| Output: |
|--------|
| WI // Watermarked Image |

**Step 1:** Partition the host image \(HI\) into non-overlapping blocks of size 2×2 pixels.

**Step 2:** Repeat Step 2.1 to Step 2.4 for each bit in the share \(S\) until all share bits are embedded.

**Step 2.1:** Apply IWT on the block (the result is LL, HL, LH, and HH).

**Step 2.2:** Make quantization to LL by using Equation (3).

**Step 2.3:** Embed one \(S\) bit in the sub-bands (LL) of each block using Equation (4)

**Step 2.4:** Apply inverse of IWT on the watermarked block.

**Step 3:** The output is WMI

The share bits are extracted from host image block by applying one level of IWT on the blocks and making quantization to the resulted LL using Eq. (3).

Finally, the bits of extracted share are obtained from the result of the quantization of LL \((q)\) using Eq. (5):

\[\text{Extracted}_\text{watermark}(i) = \mod(q, 2)\] (5)

Where \(i\) represents the index of the extracted watermark.

Algorithm 2 shows the steps of the extraction process:

**Algorithm 2: Extraction Process**

| Input: |
|--------|
| WI // Watermarked Image |

| Output: |
|--------|
| \(S\) // The share |
3. Experimental Result

The proposed algorithm is examined for different medical images, where it is coded and tested using Matlab 2018. Figure 4 shows the medical images used which are 256×256 in size and an 8-bit depth gray level MRI (Magnetic Resonance Imaging) image.

Figure 4: Secret images

Figure 4 shows a (2, 4) the scheme of the secret sharing threshold is executed on every images. Figure 5 shows the correspondent shadows. Figure 6 shows the generated shadows which are embedded in the host images. The generated stego-images are shown in Figure 7. These meaningful shadows are dispensed to four clinicians.
Figure 6: (1)-(4) Different host images (512×512).

Figure 7: (1)-(4) the generated stego shadow images (512×512)

3.1 Fidelity Measures of the Proposed Watermarking Method

The watermarking algorithm embeds the shares of 64×64 bits. The PSNR is used to evaluate the fidelity of the embedding scheme. Figure (8) shows the original and watermarked images with their PSNR values for a sample of images. The PSNR is usually used in steganography to calculate the peak signal-to-noise ratio peak in the original image and the stego image after embedding the hidden information. The following equation represents the PSNR.

\[
\text{PSNR} = 10 \log_{10} \left( \frac{R^2}{\text{MSE}} \right) \tag{6}
\]

MAX represents the maximum value of the colors, which is 255. A number means the result of the PSNR, and the measuring unit is dB [16].

| Original image | \( n \) shadows (\( n=4 \)) | Watermarked images with PSNR |
|----------------|-----------------------------|-----------------------------|
| ![Original Image](image1) | ![Shadows](image2) | 58.6512 58.7593 58.7264 57.7593 |

| Original image | \( n \) shadows (\( n=4 \)) | Watermarked images with PSNR |
|----------------|-----------------------------|-----------------------------|
Figure 8: Original image and watermarked images with their PSNR values.

The PSNR values are changed according to various factors such as data payload (share size), scaling factor and host image size used in the proposed embedding algorithm. The PSNR result is good quality. Table 1 illustrates the compression of PSNR values with some other researches in terms of PSNR and Structural similarity (SSIM). The SSIM is defined in Equation (7) [17] is a function that shows the likeness among images to the human visual system (HVS). The SSIM has values ranging between '1' and '0'. Similar images have values of SSIM closer to the value '1'.

\[
SSIM = \frac{(2\mu_{xy} + c_1)(2\sigma_{xy} + c_2)}{\mu_x^2 + \mu_y^2 + c_1(\sigma_x^2 + \sigma_y^2 + c_2)}
\]  

(7)

Table 1. The comparison of visual goodness between various methods.

| Method       | PSNR (dB) | SSIM |
|--------------|-----------|------|
| Li [18]      | 41.52     | 0.99 |
| Yuan [19]    | 51.25     | 0.99 |
| Cheng [20]   | 42.44     | 0.98 |
| He [21]      | 54.01     | 0.99 |
| Chiu [22]    | 12.84     | 0.19 |
| Maurya [23]  | 43.42     | 0.29 |
| Our Method   | 58.07     | 0.99 |
4. Conclusions

The proposed paper provides a way for sharing medical image between different clinicians depends on Thien and Lin’s Technique. The method blocks the unintentional reveling of medical data and information to any person who is not approved to see this data. N clinicians shadow, medical image and the correspondent information of EPR. Every clinician receives stego image that looks natural. EPR and the medical image is able to be restored if any k of n are collected, so before the examination or consultation, no one of the clinicians has any information or data about the any patient that his medical state can be important to the policy of the government or insurance. In addition to, this algorithm provides privacy, confidentiality, authenticity and shadow hiding. Thien and Lin’s Technique is using Polynomial coefficients that allows us to hide the secret medical image. The Embedding capacity of the secret image is larger than any other algorithm or methods in the seemliness. Furthermore, the reassembled medical image doesn’t have any distortion, so using the Steganography the Shadow images which are sends through the internet seems like any normal image.

References

[1] V. Jagannathan, A. Mahadevan, Hariharan, and Srinivasan, 2007 Number Theory Based Image compression Encryption and Application to Image Multiplexing. in IEEE - ICSCN pp.59-64.
[2] H.C. Wu, and C.C. Chang 2005 sharing visual multi-secrets using circle shares, Comput. Stand. Interfaces vol.134 pp.123–135.
[3] Peng Li, Qian Kong, Yanpeng Ma July 2014 Image Secret Sharing and Hiding with Authentication Based on PSNR Estimation, Journal of Information Hiding and Multimedia Signal Processing Vol. 5 No. 3 pp.353-366.
[4] A. Shamir 1979 How to share a secret, Communications of the ACM vol. 22 no.11, pp. 612-613.
[5] M. Naor, and A. Shamir 1995 Visual cryptography. Proc of Advances in Cryptology: Eurocrypt’94, LNCS 950 pp. 1-12.
[6] C. C. Thien, and J. C. Lin 2002 Secret image sharing, Journal of Computer & Graphics vol. 26, no. 5 pp. 765-770.
[7] J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu 2005 A new multi-secret images sharing scheme using Lagrange’s interpolation, Journal of Systems and Software vol. 76 no. 3 pp. 327-339.
[8] R. Z. Wang, and C. H. Su2006 Secret image sharing with smaller shadow images, Journal of Pattern Recognition Letters vol. 27 no. 6 pp. 551-555.
[9] Y. S. Wu, C. C. Thien, and J. C. Lin 2004 Sharing and hiding secret images with size constraint, Pattern Recognition vol. 37 no. 7 pp. 1377-1385.
[10] P. Y. Lin, J. S. Lee, and C. C. Chang 2009 Distortion-free secret image sharing mechanism using modulus operator, Journal of Pattern Recognition vol. 42 no. 5 pp. 886-895.
[11] P. Y. Lin, and C. S. Chan 2010 Invertible secret image sharing with steganography, Journal of Pattern Recognition Letters vol. 31 no.13 pp. 1887-1893.
[12] He, J., Lan, W. & Tang S. A (2017) secure image sharing scheme with high quality stego-images based on steganography. Multimed Tools Appl 76, 7677–7698 https://doi.org/10.1007/s11042-016-3429-8.
[13] Yuyuan Sun, Yuliang Lu, Jinrui Chen, Weiming Zhang, Xuehu Yan 2020 Meaningful Secret Image Sharing Scheme with High Visual Quality Based on Natural Steganography Mathematics 2020, 8, 1452; doi:10.3390/math8091452.
[14] Chiu, P.L.; Lee, K.H. 2019 Efficient constructions for progressive visual cryptography with meaningful shares. Signal Process. 165, 233–249.
[15] Maurya, R.; Kannojiya, A.K.; Rajitha, B March 2020 (Bangalore-India) An Extended Visual Cryptography Technique for Medical Image Security. In Proc. of the 2020 2nd Int. Conf. on Innovative Mechanisms for Industry Applications (ICIMIA) pp. 415–421.

[16] Hernández-Díaz, E., et al. 2021 Jpeg images encryption scheme using elliptic curves and a new s-box generated by chaos. Electronics 10(4): p. 413.

[17] Kaur, K. and E.J. Singh Reducing SSIM (Structural Similarity Index Measure) Using Improved Edge Detection Technique on Grey Scale

[18] Li, P.; Kong, Q.; Ma, Y. 2014 Image Secret Sharing and Hiding with Authentication Based on PSNR Estimation. J. Inf. Hiding Multimed. Signal Process. 5, 353–366.

[19] Yuan, H.D. 2014 Secret sharing with multi-cover adaptive steganography. Inf. Sci. 254 197–212.

[20] Cheng, T.F.; Chang, C.C.; Liu, L. 2017 secret sharing: Using meaningful image shadows based on Gray code. Multimed. Tools Appl. 76, 1–26.

[21] He, J.; Lan, W.; Tang, S. 2017 A secure image sharing scheme with high quality stego-images based on steganography. Multimed. Tools Appl. 76, 7677–7698.

[22] Chiu, P.L.; Lee, K.H. 2019 Efficient constructions for progressive visual cryptography with meaningful shares. Signal Process. 165, 233–249.

[23] Maurya, R.; Kannojiya, A.K.; Rajitha, B. 2020 (Bangalore, India.) An Extended Visual Cryptography Technique for Medical Image Security In Proce. of the 2020 2nd Int. Conference on Innovative Mechanisms for Industry Applications (ICIMIA) pp. 415–421.