Image Encryption in the Wavelet Domain

Long Bao, Yicong Zhou*, and C. L. Philip Chen

Department of Computer and Information Science, University of Macau, Macau, China

ABSTRACT

Most existing image encryption algorithms often transfer the original image into a noise-like image which is an apparent visual sign indicating the presence of an encrypted image. Motivated by the data hiding technologies, this paper proposes a novel concept of image encryption, namely transforming an encrypted original image into another meaningful image which is the final resulting encrypted image and visually the same as the cover image, overcoming the mentioned problem. Using this concept, we introduce a new image encryption algorithm based on the wavelet decomposition. Simulations and security analysis are given to show the excellent performance of the proposed concept and algorithm.

Keywords: Discrete wavelet transform , Image encryption

1. INTRODUCTION

The cloud technologies have increasing effects on the people's daily life in different ways, including cloud computing, cloud database, cloud storage and cloud collaborations. People often share personal data online and access their data in any computers. This cloud storage service is provided by several companies such as dropbox and Google drive. In general, these personal data, mainly in the form of documents, biometrics, videos and images, contain private information. With more personal data available online, providing security to these data has been an essential problem for individuals all over the world. Image encryption is a strong tool to prevent image information from leakage such that the encrypted image data cannot be decoded by the unauthorized users.

In the history of image encryption, various image encryption algorithms can be divided into two categories. One is to convert the image into an one-dimensional data matrix and then encrypt it utilizing an existing data encryption method, such as data encryption standard (DES),[1] advanced encryption standard (AES)[2] or public-key cryptography.[3] The other is to treat the original image as two-dimensional data format and encrypt it applying the discrete Fourier transform (DFT),[4–6] wave transmission,[7] chaos systems/maps[8–15] or other image encryption algorithms.[16–19] The DFT-based image encryption algorithms utilize the phase keys and system parameters to encrypt images. The algorithms have advantages in the multi-parameter selection, high speed, and parallel implementation.[6] Because chaos systems/maps have excellent properties in ergodicity, quasi-randomness and high sensitivity to initial values and parameters, they have been used for the substitution and permutation (scrambling) processes in the chaos-based image encryption algorithms. Image encryption using the wave transmission is to change the image pixel values in the way of wave transmissions.[7] Many image encryption algorithms combine the chaotic systems with other techniques of image processing. Examples include the chaos and fractional Fourier transform (FrFT),[20] as well as wave transmission and chaos.[21] All these image encryption algorithms intend to transform the original image into a noise-like encrypted image with a uniform-distributed histogram. However, the noise-like image is an apparent visual sign indicating the presence of an encrypted image. This may lead to a security problem that the encrypted images with the noise-like feature may catch people's more attentions and bring more attacks.

To address this problem, this paper applies the data hiding technology for image encryption and introduces a new concept to image encryption. It combines an encrypted original image with a cover image to generate the final encrypted image, which visually looks like the cover image. Because the final encrypted image is a normal good-looking or meaningful image, the original image is protected not only by the encryption algorithm, but also visually by the cover image. A high level of security can be achieved. To demonstrate this concept,

*Yicong Zhou: E-mail: yicongzhou@umac.mo, Telephone: +853 83978458

Mobile Multimedia/Image Processing, Security, and Applications 2013, edited by Sos S. Agaian, Sabah A. Jassim, Eliza Yingzi Du, Proc. of SPIE Vol. 8755, 875502 · © 2013 SPIE
CCC code: /13/$18 · doi: 10.1117/12.2015725

we introduces a novel image encryption algorithm based on the discrete wavelet transform (DWT). Simulation results and security analysis will be provided.

The rest of this paper is organized as follows. Section 2 will introduce the new concept of image encryption. Section 3 will introduce the DWT-based image encryption algorithm. Section 4 will present simulation results and security analysis. Finally, Section 5 will draw a conclusion.

2. THE PROPOSED CONCEPT OF IMAGE ENCRYPTION

Most existing image encryption algorithms are based on the concept of the substitution and permutation network (SPN). They intend to transform an original image into a noise-like image with a uniform-distributed histogram. As a result, the attackers have difficulty to obtain any information of the original image from the encrypted image. Let's do an interesting experiment. We put three images in Figure 1 on the Internet. People will have different responses to these images. The image in Figure 1(c) definitely brings more people's attentions because the noise-like image is an obvious sign of an encrypted image. This results in an increasing possibility that the noise-like images receive a large number of attempts of being discovered and decrypted by different users. Figures 1(a) and (b) are visually good-looking images while Figure 1(b) is an encrypted image by our algorithm proposed in Section 3. People have a high possibility of considering both images as normal images without any special attentions. This, however, will significantly reduce the possibility to be discovered and attacked because there are tons and thousands of visually good-looking images available online.

(a) (b) (c)

Figure 1. Normal and Encrypted images: (a) The original image; (b) The encrypted image by the proposed encryption algorithm in Section 3; (c) The encrypted image by the Chen's algorithm.[15]

Motivated by the data hiding technology, we propose a new concept of image encryption to overcome the above-mentioned problem. As shown in Figure 2, the proposed concept first changes the pixel locations and values in the original image by several iterative processes of the substitution and permutation (SP), and then uses an image fusion process to transform the processed original image into the final meaningful encrypted image which is visually the same as the cover image.

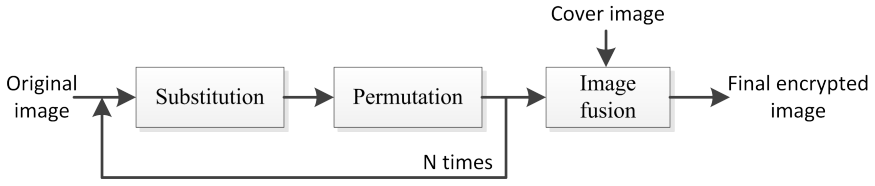


Figure 2. A new concept of image encryption

The proposed concept of image encryption ensures the security of the encrypted image with a larger key space from both the parameters of the SP process and image fusion in the following ways:

1. The final encrypted image is a visually good-looking image. The cover image can be any existing/new image which means that any image online could be the encrypted image. This keeps the encrypted image low possibility of being analyzed and attacked, achieving a higher level of security.

2. One has the difficulty to reconstruct the processed original image without knowing the method for the image fusion process and its security key which could be cover image or the parameters of image fusion.

3. To reconstruct the original image, one has to know both approaches of the image substitution and permutation and their corresponding security keys being utilized.

3. THE NEW DWT-BASED IMAGE ENCRYPTION ALGORITHM

Based on the proposed concept in Section 2, this section introduces a new DWT-based image encryption algorithm (DWT-IEA). Its block diagram is shown in Figure 3. The proposed DWT-IEA is simple and effective. It utilizes an existing image encryption algorithm to change the pixel locations and values in the original image, embeds the processed original image into a wavelet sub-band of another cover image, and applies the inverse wavelet transform to obtain the final encrypted image.

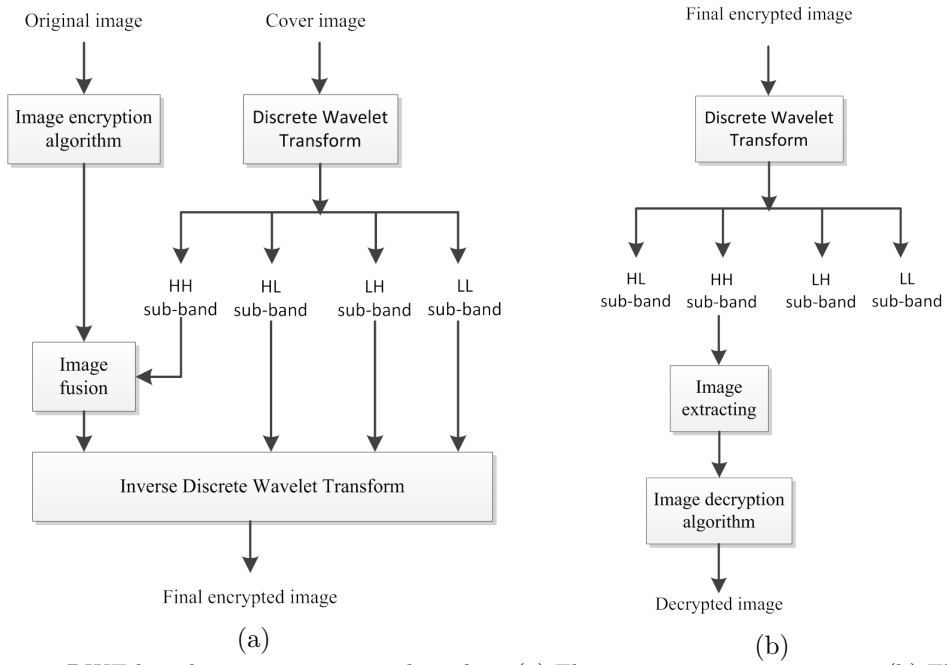


Figure 3. The new DWT-based image encryption algorithm: (a) The image encryption process; (b) The image decryption process.

To enhance the security of the final encrypted image, the proposed DWT-IEA designs an encryption process to change the pixel locations and values in the original image. The user has the flexibility to apply any image encryption algorithm for this process. As an example, this paper uses the existing CEA.[22] The CEA is based on the encryption structure of the substitution and permutation network with a high level of security withstanding different attacks.

Figure 4 shows four sub-bands of the wavelet decomposition of a grayscale image, LL, HL, LH, HH, in which L refers to low frequency while H stands for high frequency. To perform the image fusion, the proposed DWT-IEA replaces the HH sub-band of the cover image with the processed original image. The size of the cover image should be four times larger than the size of the original image. Applying the inverse wavelet transform, the DWT-IEA transforms the processed original image into the final encrypted image. Figure 5 shows the detailed results in each step in the image encryption and decryption by the proposed DWT-IEA.

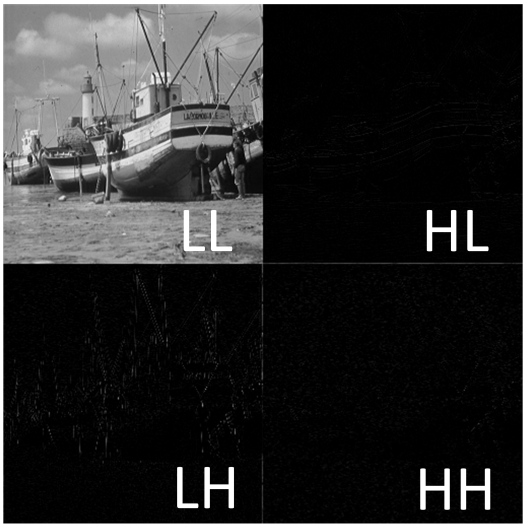


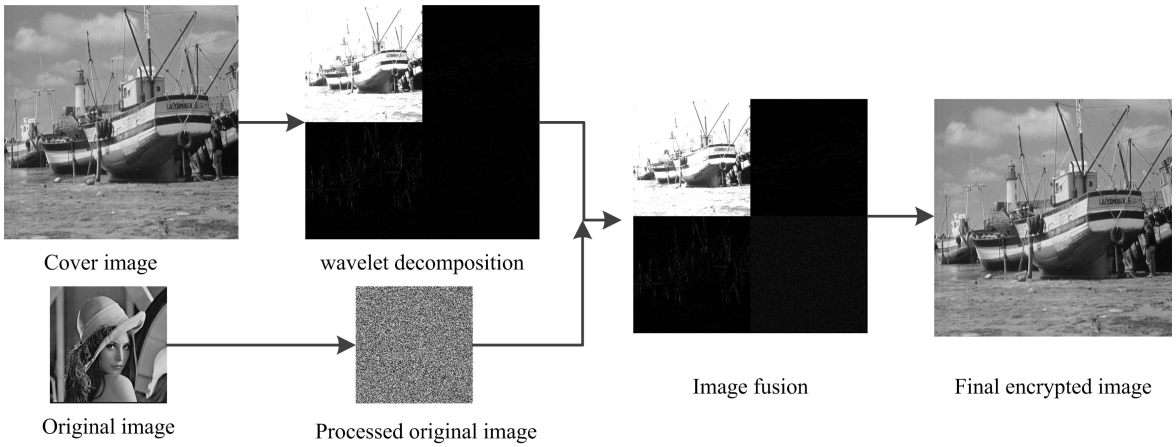
Figure 4. The wavelet decomposition results of the "boat" image

The security keys of the proposed DWT-IEA consist of two parts: (1) the type of the wavelet analysis filters being used for the wavelet decomposition of the cover image; and (2) the image encryption algorithm and its security keys. The wavelets ensure that the processed original image can be correctly extracted from the encrypted image. The later ones make sure the original image can be correctly reconstructed. They both have a large number of possible choices.

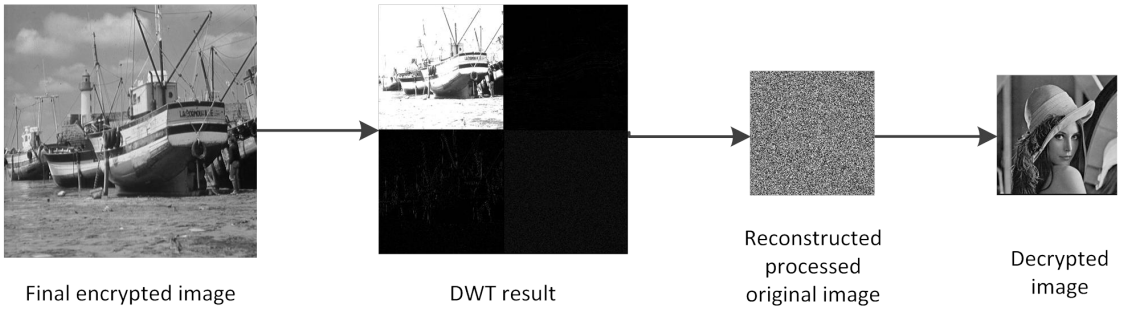
For image decryption as shown in Figure 3(b), the authorized users are provided with the correct security keys. The decryption process is also simple and effective. The encrypted image is first decomposed into four wavelet sub-bands using the correct wavelet analysis filter. After being extracted from the HH sub-band, the processed original image is then applied with the inverse process of the image encryption to reconstruct the original image. The encrypted image is a meaningful or good-looking image which is visually the same as the original cover image. Since the original cover image is not required for the image decryption process in this algorithm, it could be unknown to the public. Without knowing the original cover image, it is impossible for the attackers to check each of tons and thousands of online images to see if it is the specific image encrypted by the proposed DWT-IEA. Even if, in the worst case, the attacker is lucky enough to obtain the encrypted image. He still has difficulty to figure out the encryption algorithm and its security keys being applied to this image. These ensure the original image is protected with a high level of security.

In summary, as an example of the proposed concept, the DWT-IEA has at least four advantages:

1. Taking advantages of the data hiding technology, the DWT-IEA protects the original image in a disguising way because the encrypted image is visually a good-looking image which is the same as the cover image.
2. Its security keys are composed of the wavelet analysis filters for the cover image decomposition, and the image encryption algorithm and its security keys. Both of them have an extremely large number of possible choices, resulting in a sufficient large security key space.
3. Any encryption algorithm can be used in the encryption process for changing pixel locations and values in the original image.
4. It is extremely difficult to explore the final encrypted image in tons and thousands of good-looking images without knowing the cover image.



(a)



(b)

Figure 5. The results in each step of the proposed DWT-IEA: (a) The image encryption process; (b) The image decryption process.

4. SIMULATION AND SECURITY ANALYSIS

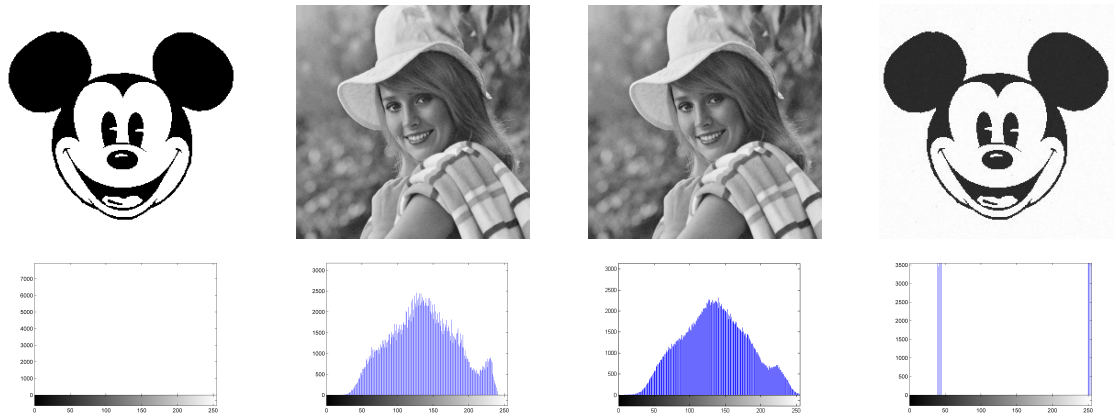
4.1 Simulation results

The new DWT-IEA can be used to encrypt different types of images, such as binary, grayscale, and color images as well as biometrics. The simulation results are shown in Figures 6-9. As can be seen, we can not visually distinguish the final encrypted images from their corresponding cover images even if their histograms have slight differences. As shown in Figure 10, different original images can be encrypted to images which are visually the same as a specific cover image. On the other hand, an original image can also be encrypted to images which are visually completely different images. Hence, any grayscale and color images can be used as the cover image for the proposed DWT-IEA. This significantly increases the attackers' difficulty of detecting the encrypted images because any online image is a potential candidate to be the encrypted image.

Due to the fact that DWTs and inverse DWTs transform image data into the double format, the forward and inverse transformation processes have data loss. As can be seen, although there are slight differences between the histograms of the decrypted and original images, they are visually the same. This is also verified by the PSNR measure results between the original image and decrypted image as shown in Table 1. Thus, little distortions by the proposed DWT-IEA can be neglected.

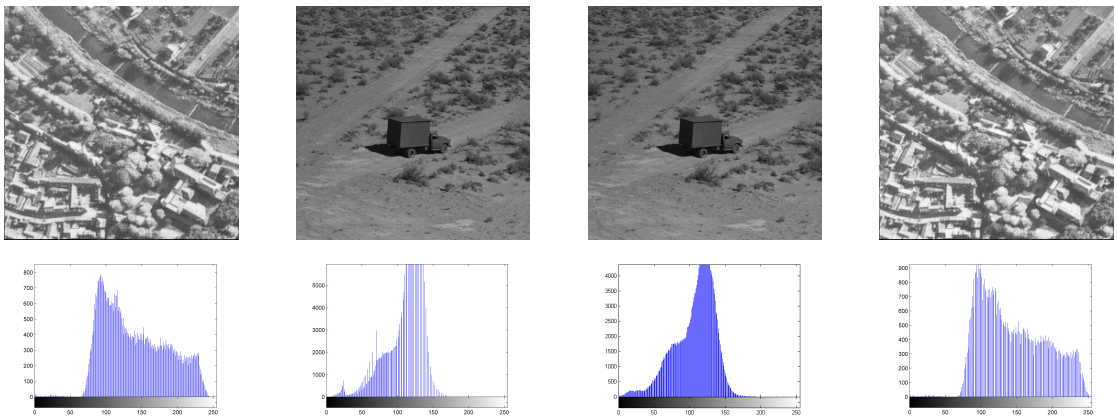
4.2 Security Analysis

The proposed DWT-IEA ensures security of the original images by combing two approaches: using an existing encryption algorithm to change pixel locations and values in the original image and applying the wavelet trans-



(a) (b) (c) (d)

Figure 6. Binary image encryption using the proposed DWT-IEA. (a) The original image; (b) The cover image; (c) The encrypted image; (d) The decrypted image.



(a) (b) (c) (d)

Figure 7. Grayscale image encryption using the proposed DWT-IEA. (a) The original image; (b) The cover image; (c) The encrypted image; (d) The decrypted image.

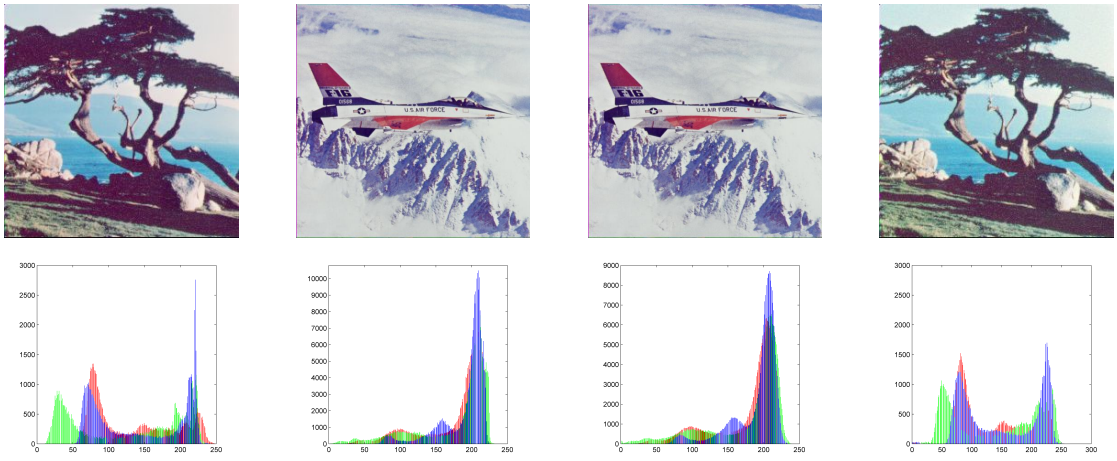
forms to embed the processed image into a cover image. The original image information is protected with a high level of security.

4.2.1 Key analysis

In the proposed DWT-IEA, any image encryption algorithm can be used for changing image pixel locations and values. Both the encryption algorithm and its security are important to reconstruct the original image. In addition, the type of wavelet analysis filters is a part of security keys. There are many different wavelet analysis filters for wavelet transform. Different wavelet analysis filters alter the wavelet decomposition results of a specific image. This leads to different encryption and decryption results. For image decryption, only the correct wavelet analysis filters can have a successful image decryption, as shown in Figure 11. Thus, the security key space of the proposed DWT-IEA is sufficiently large, withstanding the brute force attack.

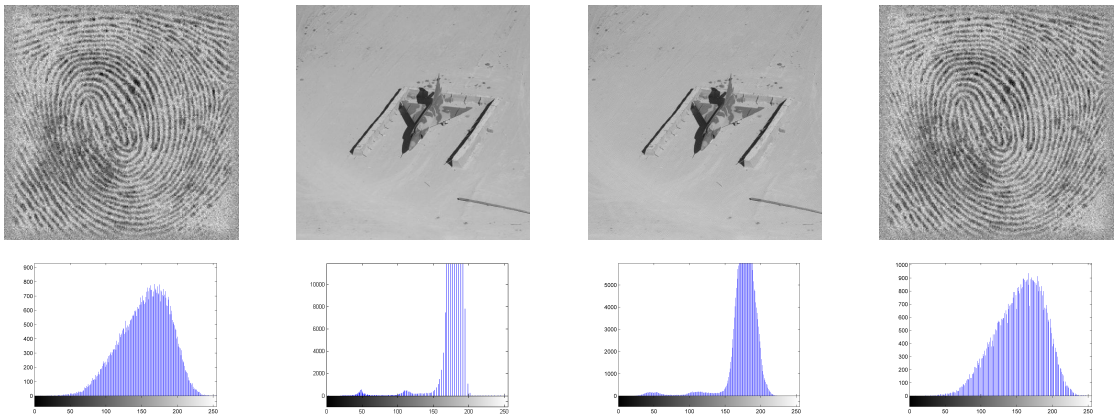
4.2.2 Similarity test

In this similarity test, peak signal-to-noise ration (PSNR) as defined in Equation (1) is selected to show how the encrypted images close to a good-looking image. The PSNR is widely used to verify the difference between two images. A higher PSNR value indicates less differences between two images.



(a) (b) (c) (d)

Figure 8. Color image encryption using the proposed DWT-IEA. (a) The original image; (b) The cover image; (c) The encrypted image; (d) The decrypted image.



(a) (b) (c) (d)

Figure 9. Biometrics encryption using the proposed DWT-IEA. (a) The original image; (b) The cover image; (c) The encrypted image; (d) The decrypted image.

(a) (b) (c) (d) (e)

Figure 10. Different encryption results. (a) The original image; (b)-(e) The encrypted images using different cover images.

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_{P_1}^2}{MSE}\right) \tag{1}$$

Where,

$$MSE = \frac{1}{WL}\sum_{i=1}^{W}\sum_{j=1}^{L}(P_1(i,j) - P_2(i,j))^2 \tag{2}$$

where P_1 and P_2 denote two images with the size of $W \times L$ and MAX_{P_1} is the maximum value of image P_1. $MAX_{P_1} = 255$ if P_1 image is a grayscale image.

Table 1. The PSNR measure results

	Cover and encrypted images	**Original and decrypted images**
	$PSNR$	$PSNR$
Figure 6	29.7298	29.2434
Figure 7	30.0484	33.8569
Figure 8	35.2572	27.9275
Figure 9	30.0570	42.9294

As seen in Table 1, the PSNR results of the images in the encryption and decryption processes in Figures 6-9 demonstrate the high similarity between the final encrypted images and their corresponding cover images. In

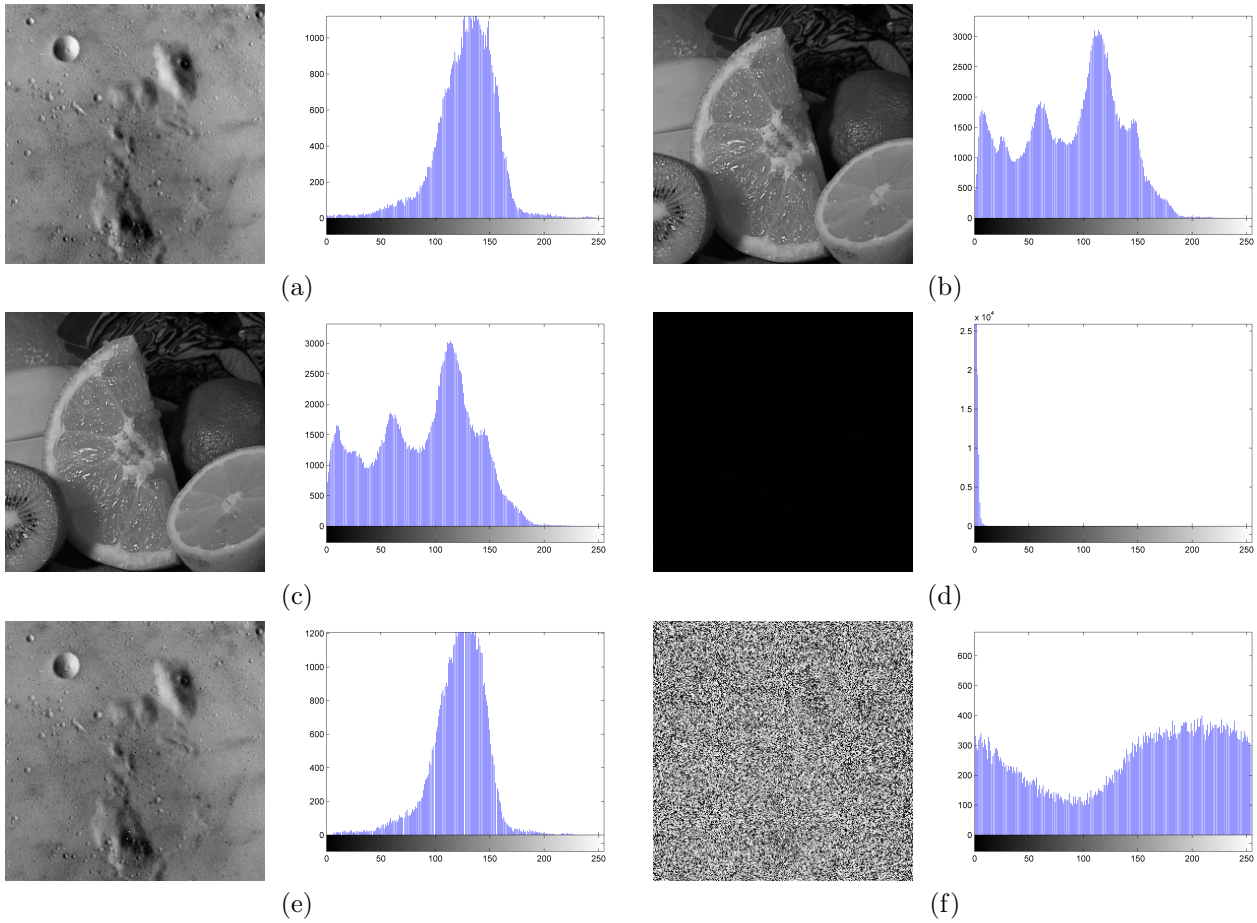


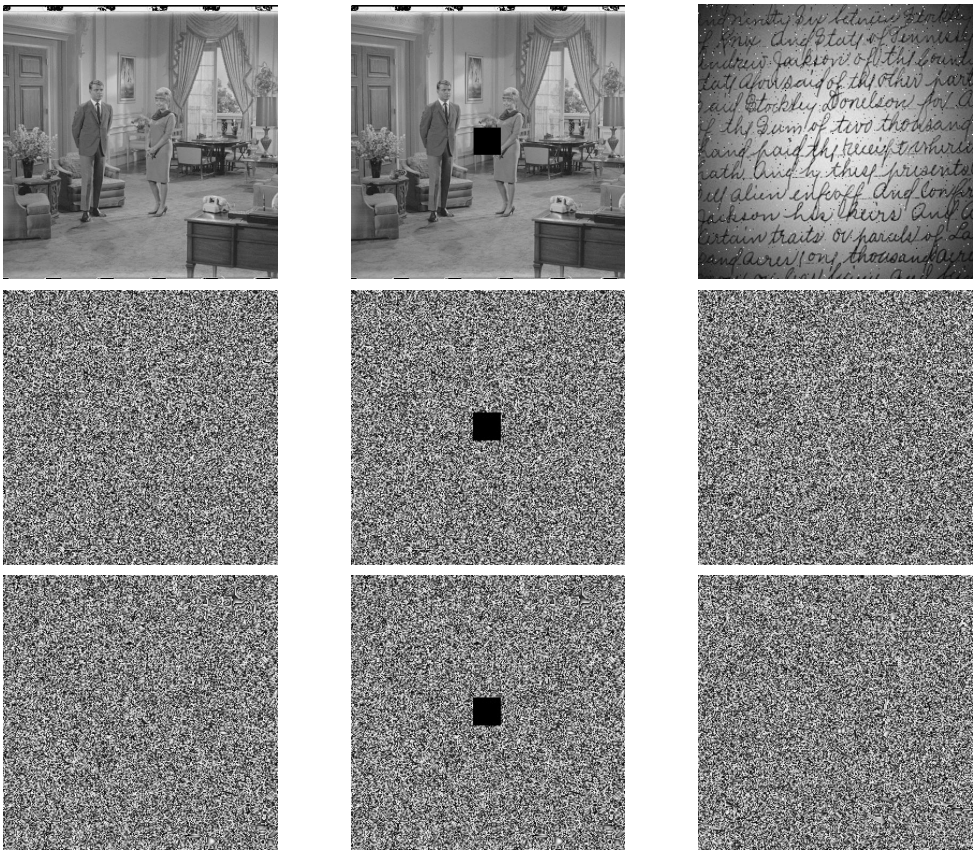
Figure 11. Image encryption and decryption using different wavelet analysis filters. (a) The original image and its histogram; (b) The encrypted image by 'db2' wavelet analysis filter and its histogram; (c) The encrypted image by 'db1' wavelet analysis filter and its histogram; (d) The difference between (b) and (C); (e) The decrypted image of (c) by 'db1' wavelet analysis filter; (f) The decrypted image of (c) by 'db3' wavelet analysis filter.

fact, it is extremely difficult to distinguish their visual differences. This indicates how an encrypted image is close to a visually meaningful image. Furthermore, the cover images are generally unknown for public. Without the original cover image as the reference, it is almost impossible for an attacker to locate our encrypted image within tons and millions of images in the public domain. Because most grayscale and color images can be used as the cover images for the proposed DWT-IEA, each image online is possible to be the encrypted image. As for tons and millions of images in the Internet, it seems impossible to check every visually meaningful image. Hence, the encrypted image by the DWT-IEA has a strong ability of camouflage.

4.2.3 Data loss attack

In the real network transmission, the image data will be separated into some data packages. If one package was lost, the traditional image encryption might fail to reconstruct the original image. For the DWT-IEA, the encrypted image with the data loss can still be decrypted successfully.

The results of data loss attacks are shown in Figure 12 in which the original image is the first image in the top row in Figure 10. Here, the top row shows the results of the DWT-IEA with a 50×50 data loss. Since the encrypted image of the DWT-IEA is four times as the original image, the data loss of the middle and bottom rows are 25×25. From the results, even with a larger data loss, the DWT-IEA successfully decrypt the encrypted image while the Wu's and Liao's algorithms fail to do so. These tests demonstrate the advantage of the DWT-IEA in the data loss attack.



(a) (b) (c)

Figure 12. The data loss attack for different image encryption algorithms. The top, middle and bottom rows are test results of the DWT-IEA, Wu's algorithm[23] and Liao's algorithm,[7] respectively. (a) The encrypted images; (b) The encrypted images with the data loss; (c) The decrypted images of (b).

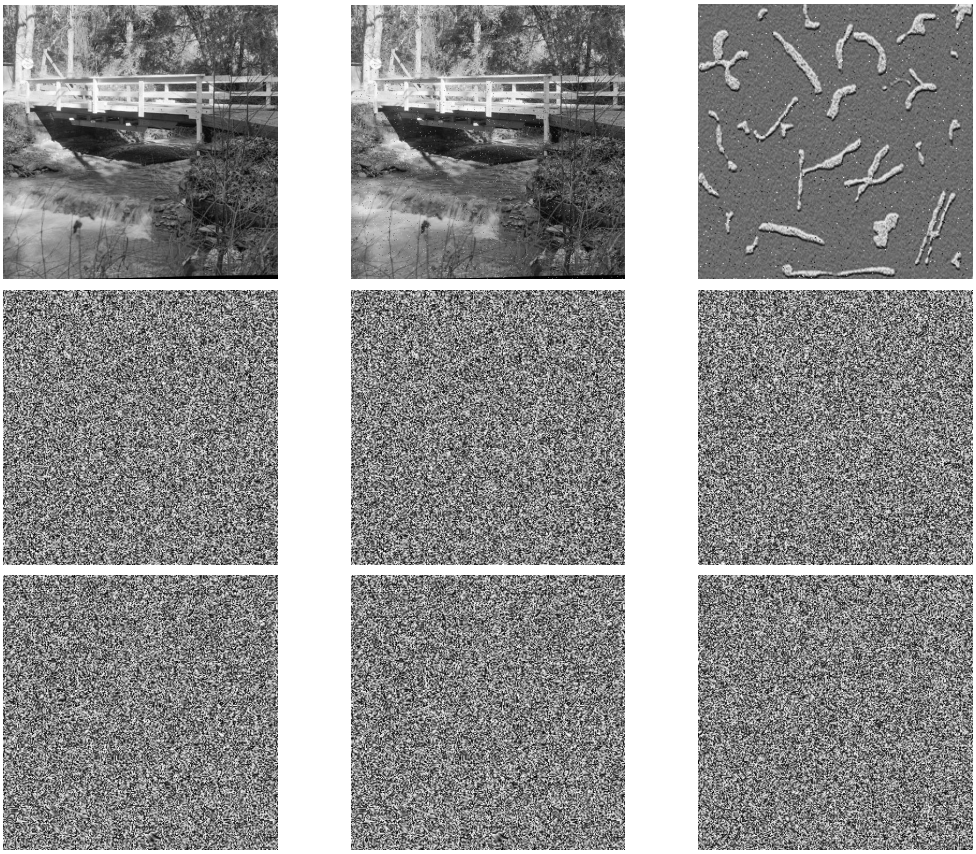
4.2.4 Noise attack

In the real applications, the transmission channels are not theoretically ideal which means that the noise will be added. If the encrypted image is added with noise, existing image encryption algorithm may not be able to reconstruct the original image correctly. But the proposed DWT-IEA can successfully decrypt the encrypted image with noise. This can be verified by the decryption results of the encrypted images with 'salt & pepper' noise for different image encryption algorithms as shown in Figure 13. The original image is the first image of the second row in Figure 10. From the results, only the DWT-IEA obtains the successful decryption result. This comparison shows the excellent performance of the DWT-IEA against the noise attack.

5. CONCLUSION

In this paper, we have introduced a new concept for image encryption. In stead of generating noise-like encrypted image, this concept is a simple and effective encryption method to transform an original image into the normal good-looking image. It encrypts the original image and then transforms it into the final meaningful encrypted image which visually looks like the cover image. The proposed encryption concept protects the original image contents both in a physical way of changing image data but also in a visually disguising way of hiding processed original image. This significantly increases the attackers' difficulty to detect and break the encrypted information.

According to the proposed encryption concept, we have also introduced a DWT-based image encryption algorithm (DWT-IEA) as an example. It embeds the processed original image into a sub-band of the wavelet decomposition of the cover image. Simulation results and security analysis have shown that the final encrypted



(a) (b) (c)

Figure 13. Noise attack for different image encryption algorithms. The top, middle and bottom rows are test results of the DWT-IEA, Wu's algorithm[23] and Liao's algorithm,[7] respectively. (a) The encrypted images; (b) The encrypted images with noise; (c) The decrypted images of (b).

image is visually the same as the cover image and the original image can be reconstructed with little invisible data loss caused by the wavelet transform. The proposed DWT-IEA is able to encrypt images with a high level of security and has excellent performance in against the data loss attack and noise attack.

6. ACKNOWLEDGE

This work was supported in part by Macau Science and Technology Development Fund under grant 017/2012/A1 and by the Research Committee at University of Macau under grants SRG007-FST12-ZYC, MYRG113(Y1-L3)-FST12-ZYC and MRG001/ZYC/2013/FST.

REFERENCES

[1] National Institute of Standards and Technology, "Data encryption standard (DES)," (1999).
[2] National Institute of Standards and Technology, "Advanced encryption standard (AES)," (2001).
[3] Rivest, R. L., Shamir, A., and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM* **21**(2), 120–126 (1978).
[4] Wang, X. and Zhao, D., "Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in fourier domain," *Optics Communications* **284**(1), 148–152 (2011).
[5] Nishchal, N. K., Joseph, J., and Singh, K., "Fully phase encryption using fractional fourier transform," *Optical Engineering* **42**(6), 1583–1588 (2003).

[6] Chang, H. T., Hwang, H.-E., and Lee, C.-L., "Position multiplexing multiple-image encryption using cascaded phase-only masks in fresnel transform domain," *Optics Communications* **284**(18), 4146–4151 (2011).
[7] Liao, X., Lai, S., and Zhou, Q., "A novel image encryption algorithm based on self-adaptive wave transmission," *Signal Processing* **90**, 2714–2722 (2010).
[8] Fu, C., Lin, B.-b., Miao, Y.-s., Liu, X., and Chen, J.-j., "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications* **284**(23), 5415–5423 (2011).
[9] Fu, C., Chen, J.-j., Zou, H., Meng, W.-h., Zhan, Y.-f., and Yu, Y.-w., "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Optics Express* **20**(3), 2363–2378 (2012).
[10] Zhu, Z.-L., Zhang, W., Wong, K.-W., and Yu, H., "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences* **181**(6), 1171–1186 (2011).
[11] Wang, X., Teng, L., and Qin, X., "A novel colour image encryption algorithm based on chaos," *Signal Processing* **92**, 1101–1108 (2012).
[12] Ye, R., "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Optics Communications* **284**(22), 5290–5298 (2011).
[13] Mao, Y. and Chen, G., [*Chaos-Based Image Encryption*], 231–265 (2005).
[14] Gao, T. and Chen, Z., "A new image encryption algorithm based on hyper-chaos," *Physics Letters A* **372**(4), 394–400 (2008).
[15] Chen, G., Mao, Y., and Chui, C. K., "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals* **21**(3), 749–761 (2004).
[16] Cao, W., Yicong, Z., and Chen, C. L. P., "A new image encryption algorithm using truncated p-fibonacci bit-planes," (October 14-17, 2012 2012).
[17] Zhou, Y., Panetta, K., and Agaian, S., "Image encryption based on edge information," in [*IS&T SPIE Electronic Imaging 2009: Multimedia on Mobile Devices 2009*], **7256**, 725603–11, SPIE (2009).
[18] Zhou, Y., Panetta, K., Agaian, S., and Chen, C. L. P., "Image encryption using p-fibonacci transform and decomposition," *Optics Communications* **285**(5), 594–608 (2012).
[19] Zhou, Y., Panetta, K., Agaian, S., and Chen, C. L., "(n, k, p)-gray code for image systems," *IEEE Trans Syst Man Cybern B Cybern* (2012).
[20] Shan, M. G., Chang, J., Zhong, Z., and Hao, B. G., "Double image encryption based on discrete multiple-parameter fractional fourier transform and chaotic maps," *Optics Communications* **285**(21-22), 4227–4234 (2012).
[21] Wang, X. Y. and Yang, L., "A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models," *Optics Communications* **285**(20), 4033–4042 (2012).
[22] Bao, L., Zhou, Y., P., C. C. L., and Liu, H., "A new chaotic system for image encryption," in [*System Science and Engineering (ICSSE), 2012 International Conference on*], 69–73 (2012).
[23] Wu, Y., Yang, G., Jin, H., and Noonan, J. P., "Image encryption using the two-dimensional Logistic chaotic map," *Journal of Electronic Imaging* **21**(1), 013014–1 (2012).