Image Encryption Using Arnold Transform Technique and Hartley Transform Domain

Kuang Tsan Lin
Department of Mechanical and Computer Aided Engineering
St. John's University
New Taipei City, Taiwan, R.O.C.
e-mail: ktlin@mail.sju.edu.tw

Abstract*—This paper proposes an image encryption method to encrypt a covert image by combining the Arnold transform technique in the space domain and the Hartley transform method in the frequency domain. First, transform a covert image into form eight binary images by decimal value to eight-digit binary operation. Then, transform eight binary images into form eight binary scrambled images by the Arnold transform, respectively. And then, recombine the sequence of the eight binary scrambled matrices into a scrambled matrix with 256 gray levels according to the specific order. Finally, derive an encrypted image from the scrambled image by the Hartley transform. Simulations show that the proposed method has higher image scrambling degree, more security and has robustness against occlusion and salt & pepper noise attacks.*

Keywords-image encryption, Arnold transform, Hartley transform

I. INTRODUCTION

Image encryption methods have two groups, one encrypts covert images in the space domain and another encrypts covert images in the frequency domain. For the first group, encrypted covert images can be retrieved with no distortion mostly. However, it is less difficulty of unauthorized people to decrypt covert images usually. Conversely, encrypted covert images in the frequency domain are with higher security, parallel and high speed processing, and it is robust for occlusion attacks and noise attacks. However, the covert images do not be exactly retrieved usually. This article will use simultaneously two groups of advantages of image encryption methods to encode a covert image.

Image scrambling techniques are greatly important image encrypting methods in the space domain. They can be used to enhance the robustness of occlusion attacks and noise attacks. They have two groups. The first group is matrix transformations, e.g. the Arnold transform [1-2]. They need correct parameters of the transformation to solve inverse of the matrix transformation. They have good security; and the decoding process of the scrambled images requires keys and the transformations are simple. The second group is coordinate movements, e.g. the cellular automata [3-4]. They also need right parameters of the scrambling path to find inverse of coordinate movement. Although the methods operate well, some distortion may be found in decoded images. This article will select the Arnold transform in the first group to scramble covert images.

Some researches assembled image scrambling techniques in the space domain and image encrypting methods in the frequency domain to increase security. Zhao *et al*. [5-6] proposed to combine image scrambling techniques and fractional Fourier transforms to encode images. Meng *et al*. [7] proposed to use image scrambling techniques and iterative Fresnel transform techniques to encode images. All the encrypting methods in the frequency domain had very good robustness, but all values in the frequency domain are complex, i.e. there are both amplitude and phase. The Hartley transformation of a real image is real as well, and it still possesses properties in the frequency domain. Therefore, this article will propose a hybrid method assembling the Arnold transform technique in the space domain and the Hartley transform in the frequency domain to possess simultaneously advantages of two domains.

II. THEORY

A. The Arnold transform techniques for scrambling images

The Arnold transform of a two-dimensional image is defined as [8]

$$A^M:\begin{bmatrix}u_i\\ v_i\end{bmatrix}=\mathrm{mod}\left(\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}\begin{bmatrix}x_i\\ y_i\end{bmatrix},M\right), \tag{1}$$

where (x_i, y_i) and (u_i, v_i) are the position coordinates of image before and after the Arnold transform. The operator "mod" is the modulus after division operation. The period p of the transform depends on the parameter M, which is the size of the image. The covert image is scrambled by the Arnold transform for iterative number n and the scrambled image can be retrieved by inverse Arnold transform for m (= p-n) and n that are keys to de-scramble the covert image.

Let $\boldsymbol{C}$ be a $r \times c$ covert image with 256-graylevel to be encoded and let $\boldsymbol{A}$ be a $r \times c$ image formed by the Arnold transform of $\boldsymbol{C}$. The processes for deriving $\boldsymbol{A}$ from $\boldsymbol{C}$ are shown below. First, transform the pixels of $\boldsymbol{C}$ into form eight binary images $\boldsymbol{B}7$, $\boldsymbol{B}6$, $\boldsymbol{B}5$, $\boldsymbol{B}4$, $\boldsymbol{B}3$, $\boldsymbol{B}2$, $\boldsymbol{B}1$, and $\boldsymbol{B}0$ by "dec2bin" operation. The operator "dec2bin" transforms a

978-0-7695-5120-3/13 $26.00 © 2013 IEEE
DOI 10.1109/IIH-MSP.2013.30

decimal value into eight digits binary values. Then, derive eight binary scrambled images $A7$, $A6$, $A5$, $A4$, $A3$, $A2$, $A1$, and $A0$ by Arnold transform. Finally, recombine the eight binary scrambled images into a scrambled image A with 256 gray levels according to the specific order. An example for the scrambling processes by the Arnold transform from a 3×3 covert image C to a 3×3 matrix A is shown in Fig. 1.

$$C=\begin{bmatrix}63 & 64 & 65\\ 127 & 125 & 123\\ 224 & 226 & 228\end{bmatrix} \quad A=\begin{bmatrix}252 & 71 & 222\\ 39 & 254 & 2\\ 190 & 130 & 7\end{bmatrix}$$

(a) (d)

$$B7=\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 1 & 1 & 1\end{bmatrix} \quad B6=\begin{bmatrix}0 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix} \quad B5=\begin{bmatrix}1 & 0 & 0\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix} \quad B4=\begin{bmatrix}1 & 0 & 0\\ 1 & 1 & 1\\ 0 & 0 & 0\end{bmatrix}$$

$$B3=\begin{bmatrix}1 & 0 & 0\\ 1 & 1 & 1\\ 0 & 0 & 0\end{bmatrix} \quad B2=\begin{bmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} \quad B1=\begin{bmatrix}1 & 0 & 0\\ 1 & 0 & 1\\ 0 & 0 & 0\end{bmatrix} \quad B0=\begin{bmatrix}1 & 0 & 1\\ 1 & 1 & 1\\ 0 & 0 & 0\end{bmatrix}$$

(b)

$$A7=\begin{bmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{bmatrix} \quad A6=\begin{bmatrix}0 & 1 & 1\\ 1 & 1 & 1\\ 1 & 1 & 1\end{bmatrix} \quad A5=\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & 0\\ 1 & 0 & 1\end{bmatrix} \quad A4=\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{bmatrix}$$

$$A3=\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{bmatrix} \quad A2=\begin{bmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 1 & 0 & 0\end{bmatrix} \quad A1=\begin{bmatrix}1 & 1 & 1\\ 0 & 1 & 0\\ 0 & 0 & 0\end{bmatrix} \quad A0=\begin{bmatrix}1 & 0 & 1\\ 0 & 1 & 0\\ 1 & 1 & 0\end{bmatrix}$$

(c)

Fig. 1 An example for the scrambling processes by the Arnold transform from a 3×3 covert matrix C to a 3×3 matrix A. (a) covert matrix C; (b) eight binary matrices $B7$, $B6$, $B5$, $B4$, $B3$, $B2$, $B1$, and $B0$; (c) eight binary scrambled matrices $A7$, $A6$, $A5$, $A4$, $A3$, $A2$, $A1$, and $A0$ using order (0, 1, 2, 3, 4, 5, 6, 7); (d) scrambled matrix A.

B. The Hartley transform methods for scrambled images

The two-dimensional Hartley transform of a real function $f(u,v)$ is defined as [9]

$$H(\xi,\eta)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}f(x,y)\cdot cas[2\pi\cdot(\xi\cdot u+\eta\cdot v)]dudv, \tag{2}$$

where $cas = cos + sin$. The inverse relation is

$$f(u,v)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}H(\xi,\eta)\cdot cas[2\pi\cdot(\xi\cdot u+\eta\cdot v)]d\xi d\eta. \tag{3}$$

Let A be a $r\times c$ scrambled matrix and a $r\times c$ encrypted matrix H is derived by the Hartley transform of the scrambled matrix. An example for the encrypting processes by the Hartley transform from a 3×3 scrambled matrix A to a 3×3 encrypted matrix H is shown in Fig. 2.

C. Image quality for the encrypted and decrypted images

To measure the image scrambling degree between $r\times c$ encrypted image H and $r\times c$ covert image C, we use the *MSE* (mean square error) of the two images H and C. The definition of the *MSE* is [8]

$$MSE=\frac{1}{r\times c}\sum_{i=1}^{r}\sum_{j=1}^{c}[\boldsymbol{H}(i,j)-\boldsymbol{C}(i,j)]^2. \tag{4}$$

A bigger *MSE* value indicates that A and H are more different.

For evaluating image quality between decoded covert image C^* and original covert image C, this paper uses the *PSNR* (peak signal to noise ratio) of the two images C^* and C. The definition of the *PSNR* is [10]

$$PSNR=10\times\log\left(\frac{M\times N}{MSE}\right). \tag{5}$$

where *MSE* is the mean square error of C and C^*.

If the *PSNR* value is higher than 30, it will be difficult to see the difference between C and C^* for naked eyes; i.e. the image C^* looks almost the same as the image C [11].

$$A=\begin{bmatrix}252 & 71 & 222\\ 39 & 254 & 2\\ 190 & 130 & 7\end{bmatrix} \quad H=\begin{bmatrix}1167.0 & 332.0 & -56.0\\ 206.3 & -482.9 & 296.9\\ 261.7 & 75.1 & 467.9\end{bmatrix}$$

(a) (b)

Fig. 2 An example for the encrypting processes by the Hartley transform from a 3×3 scrambled matrix A to a 3×3 encrypted matrix H. (a) scrambled matrix A; (b) encrypted matrix H.

III. SIMULATIONS

Fig. 3 shows a 256×256 256-graylevel picture used as the covert image C for test.

Fig. 3 The 256×256 covert image C with 256-graylevel for test.

The test about the covert image C in Fig. 3 is introduced below. Firstly, since the gray levels of C is 256, transform the pixels of C into form eight binary images $B7$, $B6$, $B5$, $B4$, $B3$, $B2$, $B1$, and $B0$ by "dec2bin" operation. The eight binary images are shown in Fig. 4. Secondly, derive eight binary scrambled images $A7$, $A6$, $A5$, $A4$, $A3$, $A2$, $A1$, and $A0$ by the Arnold transform respectively from $B7$, $B6$, $B5$, $B4$, $B3$, $B2$, $B1$, and $B0$. The eight binary scrambled images are shown in Fig. 5. Thirdly, recombine the sequence of the eight binary scrambled matrices into a scrambled matrix A with 256 gray levels as shown in Fig. 6. Finally, derive a 256×256 encrypted image H from the 256×256 scrambled image A by the Hartley-transform. The encrypted image is shown as Fig. 7.

The above processes are used to encrypt the covert image C in Fig. 3. (1) Use C to form $B7$, $B6$, $B5$, $B4$, $B3$, $B2$, $B1$, and $B0$ by "dec2bin"; (2) $B7$, $B6$, $B5$, $B4$, $B3$, $B2$, $B1$, and $B0$ are used to form $A7$, $A6$, $A5$, $A4$, $A3$, $A2$, $A1$ and $A0$ by the Arnold transform; (3) combine $A7$, $A6$, $A5$, $A4$, $A3$, $A2$, $A1$ and $A0$ to form A; (4) use A to form H by the Hartley transform. Conversely, the decrypting processes are below. (1) use H to form A^* by inverse Hartley transform; (2) use A^* to form $A7^*$, $A6^*$, $A5^*$, $A4^*$, $A3^*$, $A2^*$, $A1^*$ and $A0^*$ by "dec2bin"; (3) $A7^*$, $A6^*$, $A5^*$, $A4^*$, $A3^*$, $A2^*$, $A1^*$ and $A0^*$ are used to form $B7^*$, $B6^*$, $B5^*$, $B4^*$, $B3^*$, $B2^*$, $B1^*$, and $B0^*$; (4) use $B7^*$, $B6^*$, $B5^*$, $B4^*$,

$\boldsymbol{B}3^*$, $\boldsymbol{B}2^*$, $\boldsymbol{B}1^*$, and $\boldsymbol{B}0^*$ are used to form $\boldsymbol{C}^*$. We do not show the decrypting processes again, since the images retrieved in the decrypting processes are all the same as the images derived in the encrypting ones.

The *MSE* value between the covert image $\boldsymbol{C}$ and the scrambled image $\boldsymbol{A}$ is 4.12×10^3. And the *MSE* value between the covert image $\boldsymbol{C}$ and the encrypted image $\boldsymbol{H}$ is 1.12×10^9. Therefore, $\boldsymbol{H}$ is more different than $\boldsymbol{A}$ based on the covert image $\boldsymbol{C}$. The *PSNR* value between the original covert image $\boldsymbol{C}$ and the decrypted covert image $\boldsymbol{C}^*$ is nearly infinity by computer simulations for the case of the covert image. Therefore, the two images $\boldsymbol{C}$ and $\boldsymbol{C}^*$ look almost identical for the case. There is almost no distortion during the covert image decryption. The decrypted covert image $\boldsymbol{C}^*$ is shown in Fig. 8.

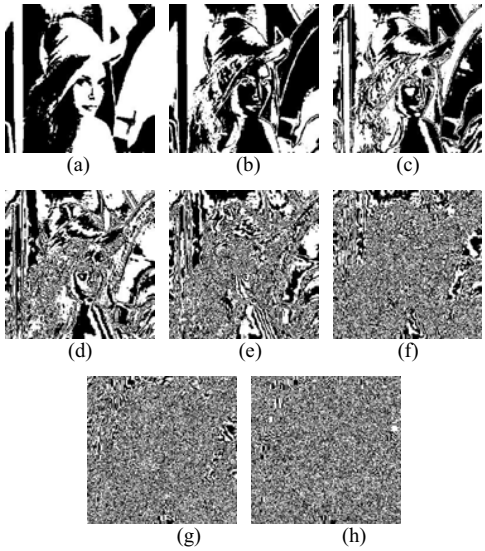


Fig. 4 Binary images (a) $\boldsymbol{B}7$; (b) $\boldsymbol{B}6$; (c) $\boldsymbol{B}5$; (d) $\boldsymbol{B}4$; (e) $\boldsymbol{B}3$; (f) $\boldsymbol{B}2$; (g) $\boldsymbol{B}1$; (h) $\boldsymbol{B}0$.

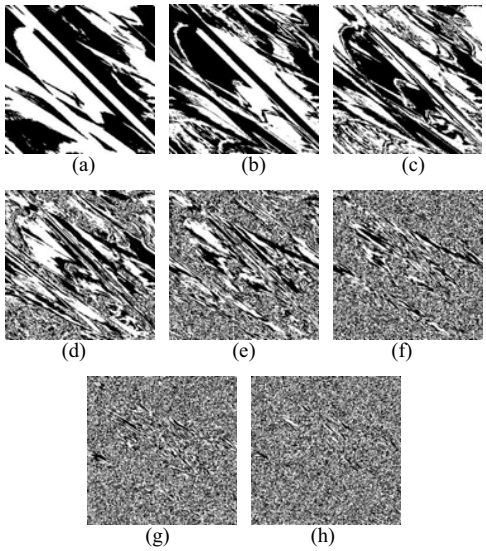


Fig. 5 Binary scrambled images (a) $\boldsymbol{A}7$; (b) $\boldsymbol{A}6$; (c) $\boldsymbol{A}5$; (d) $\boldsymbol{A}4$; (e) $\boldsymbol{A}3$; (f) $\boldsymbol{A}2$; (g) $\boldsymbol{A}1$; (h) $\boldsymbol{A}0$.

Fig. 6 The scrambled matrix $\boldsymbol{A}$.

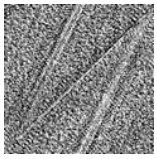


Fig. 7 The encrypted image $\boldsymbol{H}$.

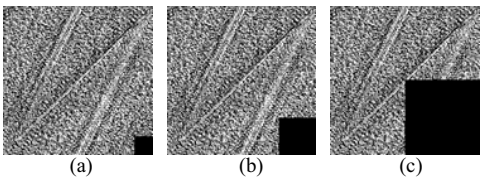
Fig. 8 The decrypted covert image $\boldsymbol{C}^*$.

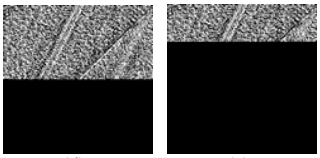
IV. DISCUSSION

The image quality of the retrieved image depends on the period of the Arnold transform, the iterative number, and the order of recombining the eight binary images. For example, combine $\boldsymbol{A}7$, $\boldsymbol{A}6$, $\boldsymbol{A}5$, $\boldsymbol{A}4$, $\boldsymbol{A}3$, $\boldsymbol{A}2$, $\boldsymbol{A}1$ and $\boldsymbol{A}0$ to form $\boldsymbol{A}$ in the encrypting process according to the order is (0, 1, 2, 3, 4, 5, 6, 7). Then select the wrong order (7, 1, 2, 3, 4, 5, 6, 0) in the decrypting process. The decrypted covert image $\boldsymbol{C}^*$ is shown in Fig. 9, and the *PSNR* value between the original covert image $\boldsymbol{C}$ and the decrypted covert image $\boldsymbol{C}^*$is 9.1.

Fig. 9 The decrypted covert image $\boldsymbol{C}^*$ with a wrong order (7, 1, 2, 3, 4, 5, 6, 0).

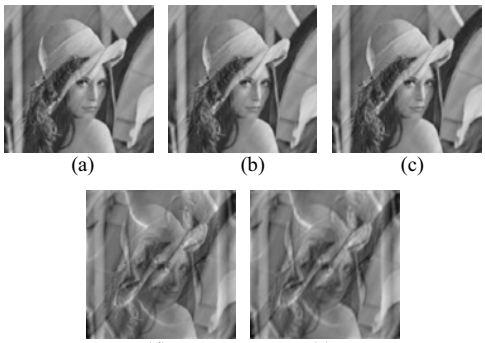
The robustness of the proposed method is verified against occlusion attacks on the encrypted image with 1/64, 1/16, 1/4, 1/2, and 3/4 occlusion size as shown in Fig. 10(a)-10(e), respectively, and their corresponding decrypted images are display in Fig. 11(a)-11(e), respectively. The *PSNR* values between original covert images and their corresponding decrypted images with correct keys from the encrypted image with 1/64, 1/16, 1/4, 1/2, and 3/4 occlusion size are = 32.6, 32.6, 32.3, 18.9, and 18.2, respectively. The decrypted images having some occlusion are recognizable.





(d) (e)

Fig. 10 The encrypted images with (a) 1/64; (b) 1/16; (c) 1/4; (d) 1/2; (e) 3/4 occlusion size.

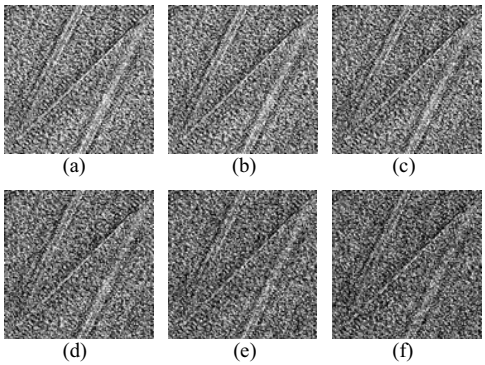


(a) (b) (c)

(d) (e)

Fig. 11 The decrypted images with (a) 1/64; (b) 1/16; (c) 1/4; (d) 1/2; (e) 3/4 occlusion size of the encrypted images.

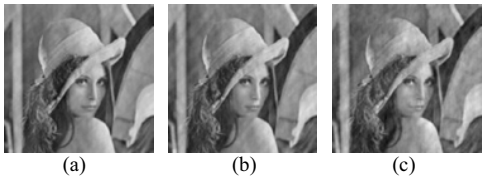
The robustness is also tested against salt & pepper noise attack on the encrypted images with density of 0.05, 0.1, 0.2, 0.3, 0.4, and 0.5, as shown in Fig. 12(a)-12(f), respectively, and the corresponding decrypted images are shown in Fig. 13(a)-13(f), respectively. The *PSNR* values between original covert images and their corresponding decrypted images with correct keys from the encrypted image with salt & pepper noise having density of 0.05, 0.1, 0.2, 0.3, 0.4, and 0.5 are = 31.3, 31.0, 26.6, 26.0, 22.1, and 20.5, respectively. The decrypted images having some noise are also recognizable. The proposed method has robustness against occlusion and noise attacks.



(a) (b) (c)

(d) (e) (f)

Fig. 12 The encrypted images with density of (a) 0.05; (b) 0.1; (c) 0.2; (d) 0.3; (e) 0.4; (f) 0.5.



(a) (b) (c)

(d) (e) (f)

Fig. 13 The decrypted images with density of (a) 0.05; (b) 0.1; (c) 0.2; (d) 0.3; (e) 0.4; (f) 0.5 of the encrypted images.

V. CONCLUSION

The proposed method can encrypt a covert image by assembling the Arnold transform technique in the space domain and the Hartley transform method in the frequency domain. The encrypted image has more different than the scrambled image only by the Arnold transform. The image quality of the decrypted image depends on the period of the Arnold transform, the iterative number, and the order of recombining eight scrambled binary images so the proposed method is more security. The proposed method has robustness against occlusion and salt & pepper noise attacks.

REFERENCES

[1] Y. L. Yang, N. Cai, and G. Q. Ni, "Digital image scrambling technology based on the symmetry of Arnold transform," Journal of Beijing Institute of Technology **15** (2006) 216.

[2] B. Li and J. W. Xu, "Period of Arnold transformation and its application in image scrambling," Journal of Central South University of Technology **12** (2005) 278.

[3] O. Lafe, "Data compression and encryption using cellular automata transforms," Engineering Application of Artificial Intelligence **10** (1997) 581.

[4] G. Z. Hernandez and H. J. Herrmann, "Cellur automata for elementary image enhancement," Graphical Models and Image Processing **58** (1996) 82.

[5] J. Zhao, H. Lu, X. Song, J. Li, and Y. Ma, "Optical image encryption based on multistage fractional Fourier transforms and pixel scrambling technique," Optics Communications **249** (2005) 493.

[6] J. Zhao, H. Lu, and Q. Fan, "Color image encryption based on fractional Fourier transforms and pixel scrambling technique," Proceedings of SPIE **6279** (2007) 62793B.

[7] X. F. Meng, L. Z. Cai, X. L. Yang, X. X. Shen, and G. Y. Dong, "Information security system by iterative multiple-phase retrieval and pixel random permutation," Applied Optics **45** (2006) 3289.

[8] M. R. Abuttrab, "Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain," Optics & Laser Technology 45 (2013) 525-532.

[9] R. N. Bracewell, H. Bartelt, A. W. Lohmann, and N. Streibl, "Optical synthesis of the Hartley transform," Applied Optics 24 (1985) 1401-1402.

[10] M. Kutter and F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," Proceedings of SPIE **3657** (1999) 226.

[11] T. K. Shih, L. C. Lu, and R. C. Chang, "An automatic image in paint tool," Proceedings of the Eleventh ACM International Conference on Multimedia (2003) 102.