Medical Image Encryption Scheme Based on Arnold Transformation and ID-AK Protocol

Osman Wahballa[1,2], Abubaker Wahaballa[1], Fagen Li[1], Idris Ibn Idris[3] and Chunxiang Xu[1]
(Corresponding author: Abubaker Wahaballa)

University of Electronic Science and Technology of China, Chengdu, China[1]
(Email: wahaballah@hotmail.com)
Karary University, Khartoum, Sudan[2]
Modibbo Adama University of Technology, Yola, Nigeria[3]

(Received May 10, 2016; revised and accepted Sept. 3 & Oct. 6, 2016)

Abstract

Providing security on transmitted medical image over public channels has become an essential part of computer-aided diagnosis systems. In this paper, we propose an efficient image encryption scheme for medical applications based on Arnold transformation and pairing-free identity-based authenticated key agreement protocol. This allows user to send and receive medical images over public channel safely, while maintaining patient privacy. We then provide the numerical analysis results to prove the robustness of our scheme. These results are carried out via both theoretic analysis and experimental simulations based on MATLAB . The analysis demonstrates that our scheme meets the effectiveness and security requirements of image encryption.

Keywords: Arnold Transformation; Identity (ID)-based Cryptography; Medical Image Encryption Scheme; Statistical Attack

1 Introduction

Image-based diagnostics has become an effective tool for the treatment and prediction of many diseases. In healthcare system, the medical images can be transmitted across public channels such as the Internet. However, these images contain very sensitive and confidential information. Therefore, maintaining security and confidentiality of medical images is of utmost priority. Most of the current medical images protection techniques use symmetric encryption [2, 4, 34], traditional public key cryptography [17, 32] or watermarking [13, 19]. However, symmetric encryption suffers from the problem that the same key must be shared by the sender and the receiver and traditional PKC has a complex certificate management, while watermarking is lacking of a standard attack benchmark and distortion measurement [28]. Image encryption techniques are classified based on both spatial and frequency domain [30]. Arnold transformation has been adopted in a wide variety of multimedia securities because of its periodicity.

Identity(ID)-based cryptography aims to simplify the complex certificate management in the traditional PKC by deriving user's public key from his/her identity. The major advantage of IBC is that it does not require the use of digital certificates to guarantee the authenticity [29]. *Key-agreement protocol* is process whereby two or more parties can establish a shared secret key in such a way that both sides agree with the outcome. Identity-based authenticated key agreement is a useful cryptographic primitive and has been widely used in various applications. In cryptography, bilinear pairing is a mathematical function which combine elements of two cryptographic groups to a third group. Bilinear pairing is widely used to construct or analyze various kinds of authenticated key agreement protocols. However, a bilinear pairing operation is more time-consuming than other operations over elliptic curve group.

In this paper, we propose an encryption scheme for the medical image by incorporating the idea of identity-based authenticated key agreement and Arnold transformation.

1.1 Motivations

Providing security on transmitted medical image has become more and more important with rapid development of both image-based diagnostics techniques and Internet in the field of medical informatics. Furthermore, Health Insurance Portability and Accountability Act (HIPAA) [23] issued mandates for ensuring privacy and security of electronic health information, where healthcare providers are obliged to take appropriate safeguards and measures to ensure that patient information is only provided to people who have a professional need. To reap the benefits of ehealth by achieving better health outcomes, and to improve healthcare quality and efficiency, healthcare providers and patients alike must trust that the patient's health information is private and secure. The goal of this work is to create an encryption scheme for the medical image by combining identity-based encryption with and an Arnold transformation.

In a nutshell, our contribution is threefold:

- An efficient encryption scheme for the medical image from identity-based encryption is presented that allows user to send and receive medical images over public channels safely, while maintaining patient's privacy and confidentiality.
- A pairing-free identity-based key exchange protocol for medical image encryption is introduced.
- Numerical analysis results are carried out to prove the robustness of our scheme. The analyses demonstrate that our scheme meets the effectiveness and security requirements of image encryption.

The remainder of this paper is organized as follows. In the next section, the state-of-the-art is discussed. Section 3 presents the preliminaries of this paper. The proposed scheme is introduced and discussed in Section 4, while Section 5 is devoted to experimental results. Finally, we conclude the paper in Section 6.

2 State-of-the-Art

Nowadays designing a secure and efficient encryption schemes is a crucial issue for digital image encryption. Due to the large image size, conventional cryptosystems are widely used, such as RSA [22], however, it cannot easily be directly used for image encryption. Instead of the above solution, some researchers focus on designing symmetric image cryptosystems. In particular, a number of schemes [5, 8, 9, 12, 21, 25, 26, 33], based on chaos have been proposed. The chaos-based cryptosystems has some inherent features, such as sensitivity to initial condition and pseudo randomness, therefore, this solution appear more suitable for high-security encryption. Nevertheless, chaos-based schemes have their own weaknesses in terms of exchanging and distributing the symmetric secret keys. This is a particularly serious problem due to the large number of users. In addition, the solution based on chaos-based cryptosystems may have unknown vulnerabilities. Recently several image encryption algorithms founded on chaos have been broken [1, 15, 16, 24]. For instance, an encryption scheme based on improved hyper chaotic sequences is addressed by C. Zhu [33]. Their scheme used a four-dimensional hyper-chaos system in order to generate a pseudo-random number sequence. Later the sequence is applied to control the modulation addition and the bitwise exclusive OR operation. C. Li et al. [16] analyzed that; if two known plain-images and the corresponding cipher-images are available this scheme can be easily broken. Ideally, in order to avoid these problems a public key encryption is highly recommended. The public key encryption for large image based on elliptic curve is considered by L. Chen et al [6].

3 Preliminaries

In this section, we describe the basic definitions and assumptions that are used in our scheme.

3.1 Elliptic Curves Cryptography (ECC)

The ECC was proposed by Miller and Koblitz [14, 18] as an alternative to RSA in public key cryptography. Any cryptosystem based on ECC provides high security with small key size, for example, a 160-bit ECC is considered to be as secured as 1024-bit RSA key [11]. Let F_q be a field of integers of a modulo a large prime number q. A non-singular elliptic curve $E_q(a, b)$ over F_q is defined by the following equation

$$y^2 \bmod q = (x^3 + ax + b) \bmod q, \tag{1}$$

where $a, b, x, y \in F_q$ with the discriminant $\triangle = (4a^2 + 27b^2) \bmod q \neq 0$. A point $P(x, y)$ is an elliptic curve point if it satisfies Equation (1), and the point $Q(x, -y)$ is called the negative of P, i.e. $Q = -P$. The points $E_q(a, b)$ together with a point $\mathcal{O}$ (called point at infinity) form an additive cyclic group G_q, that is, $G_q = \{(x, y) : a, b, x, y \in F_q \text{ and } (x, y) \in E_q(a, b)\} \bigcup \{\mathcal{O}\}$ of prime order q. Scalar multiplication over $E|F_q$ can be computed as follows:

$$tP = P + P + ... + P \quad (t \quad times). \tag{2}$$

3.2 Arnold Transformation

The Arnold transformation, also referred to as cat map, is one of the images scrambling techniques that was named after the Russian mathematician Vladimir Arnold, who demonstrated its effectiveness in image processing. The Arnold transformation is periodic, besides it can only be used with square images. The general form of Arnold transformation appears in Equation (3). This equation can be adopted for digital images as follows. Let (i, j) be pixel for $N \times N$ digital image $Img[i][j]$. This image is transformed to $Img[i'][j']$ using Equation (3). As mentioned, Arnold transformation is periodic with period T that depends on the size of the images. Due to the periodicity equation 3 is applied 3 in both scrambling as descrambling processes. If the Arnold is applied (t) times to yield a scrambled image in the sender side, it should be applied $(T - t)$ times to yield the original image in the receiving side. Arnold transformation period T is given by Equation (4) [10, 31].

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \bmod N \tag{3}$$

$$T = 1.4938N + 40.8689, \quad \text{where} \quad 2 \leq N \leq 2000 \tag{4}$$

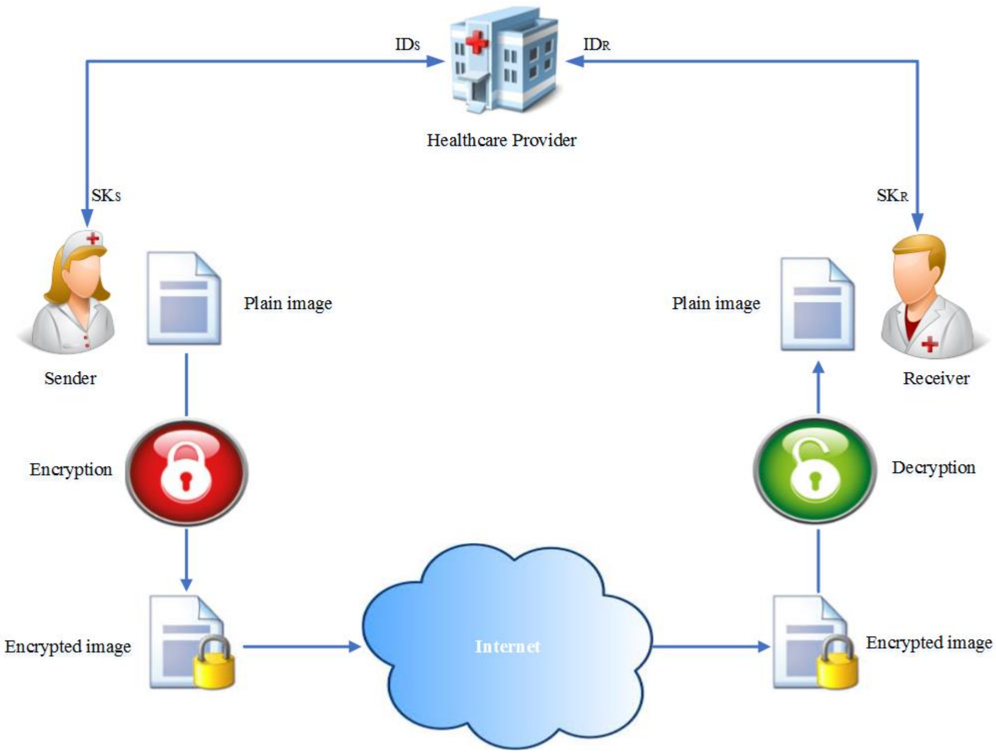


Figure 1: System structure

Table 1: Notations of our model

$\mathcal{HP}$	Healthcare Provider
$\mathcal{S}$	Sender
$\mathcal{R}$	Receiver
PP, $S_\circ$	Public Parameters and Master Key
ID_S	Sender's Identity
ID_R	Receiver's Identity
SK_S	Sender's secret key
SK_R	Receiver's secret key
sk	Shared secret key
Img_ρ	A plain medical image
Img_ϕ	An encrypted medical image
H_1, H_2	Two hash functions

4 Proposed Scheme

4.1 Overview of Our Scheme

In this section, we describe our scheme in the high level. The proposed scheme consists of three entities: a sender $\mathcal{S}$, receiver $\mathcal{R}$ and healthcare provider $\mathcal{HP}$. $\mathcal{HP}$ is adopted as trusted third party in our scheme. It is responsible to initialize the public system parameters. In order to establish a secure communication channel between $\mathcal{S}$ and $\mathcal{R}$, we employ identity-based key exchange protocol [3].

The interaction scenario between the above entities is divided into four phases: *Setup and Registration Phase*, *Key Agreement Phase*, *Encryption Phase* and *Decryption Phase*. Figure 1 shows the sketch of the interaction scenario.

In the setup and registration phase, $\mathcal{HP}$ inputs the security parameters as defined in Section 3.1. Then, it generates the public parameters *params* and a master key s. Further, sender $\mathcal{S}$ and receiver $\mathcal{R}$ with identities ID_S and ID_R register at $\mathcal{HP}$. Afterward, $\mathcal{HP}$ generates sender's and receiver's secret keys, SK_S and SK_R respectively. In key agreement phase, $\mathcal{S}$ and $\mathcal{R}$ establish an authenticated session key. Using the shared secret key K and Arnold transformation, the sender $\mathcal{S}$ encrypts a plain medical image IMG_p to get an encrypted image IMG_c, and finally sends it over Internet to the receiver $\mathcal{R}$. Upon receiving the encrypted image IMG_c, $\mathcal{R}$ uses the shared secret sk to decrypt it.

For convenience, the notations of the proposed scheme are defined in Table 1.

4.2 Concrete Construction

In this section, we concretely construct a medical image encryption scheme by incorporating Arnold transformation and identity-based key exchange protocol. The proposed scheme is composed of the following phases.

4.3 Setup and Registration Phase

4.3.1 Setup

Initially, $\mathcal{HP}$ inputs the security parameters k and determines the tuple $\{F_q, E|F_q, G, P\}$ as defined in Section 3.1. Then, it picks secret master key $\alpha \in \mathbb{Z}_q^*$ and computes its public master-key $S_\circ = \alpha P$. Afterward, $\mathcal{HP}$ chooses two hash functions $H_1 : \{0,1\}^* \times G \to \mathbb{Z}_q$ and $H_2 : \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \times G \to \{0,1\}^k$. Finally, the $\mathcal{HP}$ publishes the system parameters: $\mathsf{PP} = (F_q, E|F_q, G, P, S_\circ, H_1, H_2)$.

4.3.2 Registration

The sender $\mathcal{S}$ with identity ID_S and receiver $\mathcal{R}$ with identity ID_R register at $\mathcal{HP}$. Given user's identity ID_i, public parameters PP and public master key $S_\circ$, $\mathcal{HP}$ picks $r \in \mathbb{Z}_q^*$, and computes $R_i = rP$ and $H_1(ID_i||R_i)$. Then, it computes $S_i = r + h_i\alpha$. The $\mathcal{HP}$ sets the pair (S_i, R_i) as user's long-term private key. The pair (S_i, R_i) is transmitted to the user U_i secretly. U_i check if $S_iP = R_i + H_1(ID_i||R_i)S_\circ$ holds. If it does, the long-term private key is valid, reject otherwise.

4.4 Key Agreement Phase

In this phase, sender $\mathcal{S}$ and receiver $\mathcal{R}$ establish an authenticated session key as follows.

Step 1: $\mathcal{S}$ chooses at random the ephemeral key $s \in_R \mathbb{Z}_q^*$ and computes the key token $T_S = sP$.

Step 2: $\mathcal{S}$ sends $M_S = (R_S, T_S, ID_S)$ to $\mathcal{R}$.

Step 3: Upon $\mathcal{R}$ receiving M_S, he chooses $\mathcal{R}$'s ephemeral key $r = \in_R \mathbb{Z}_q^*$ and computes the key token $T_R = rP$.

Step 4: $\mathcal{R}$ sends $M_R = (R_R, T_R, ID_R)$ to $\mathcal{S}$.

Step 5: Then, both sides can compute the shared secrets as follows:

- $\mathcal{S}$ computes

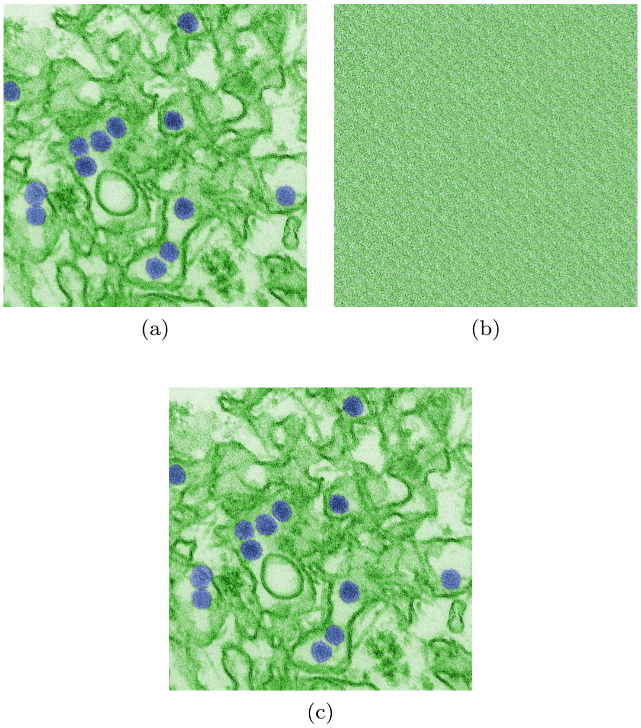
$$\begin{aligned} K_{SR}^1 =& S_ST_R + s(R_R + H_1(ID_R||R_R))S_\circ \\ \textit{and } K_{SR}^2 =& sT_R. \end{aligned}$$

- $\mathcal{R}$ computes

$$\begin{aligned} K_{RS}^1 =& S_RT_S + r(R_S + H_1(ID_S||R_S))S_\circ \\ \textit{and } K_{RS}^2 =& rT_S. \end{aligned}$$

Step 6: Eventually, $\mathcal{S}$ and $\mathcal{R}$ can compute the shared secret keys as:

$$\begin{aligned} sk &= H_2(ID_S||ID_R||T_S||T_R||K_{SR}^1||K_{SR}^2) \\ &= H_2(ID_S||ID_R||T_S||T_R||K_{RS}^1||K_{RS}^2). \end{aligned}$$



(a) (b) (c)

Figure 2: (a) Zika virus original image; (b) Zika virus encrypted image; (c) Zika virus decrypted image.

4.5 Encryption Phase

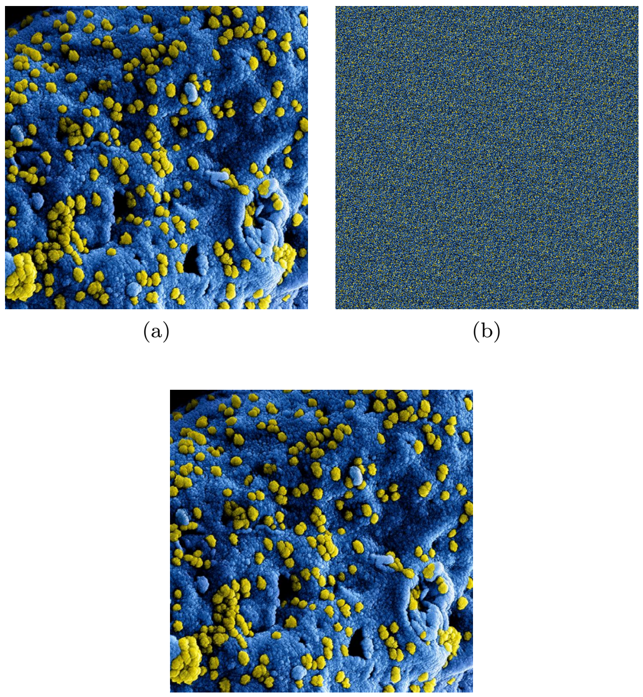
In this phase, sender $\mathcal{S}$ encrypts a plain medical image Img_ρ using the shared secret key and Arnold transformation algorithm to get the encrypted image Img_ϕ as: $Img_\phi = \Phi_{sk}(Img_\rho)$, where Φ is the Arnold transformation scrambling algorithm. The pseudo-code of scrambling process is illustrated in Algorithm 1. From steps 1-5, algorithm parameters are initialized. We perform scrambling process in steps 6-13 within Arnold transformation period T. In steps 14-21, we calculate best scrambling iteration Bst_τ, which has a minimum correlation coefficient. The Bst_τ is used as descrambling period in the next phase.

4.6 Decryption Phase

Upon receiving the encrypted image Img_ϕ from the sender $\mathcal{S}$, receiver $\mathcal{R}$ uses the shared secret key sk and Arnold transform descrambling algorithm to decrypt the Img_ϕ as: $Img_\rho = \Psi_{sk}(Img_\phi)$. where Ψ is the Arnold transformation descrambling algorithm. Due to the periodicity of Arnold transformation, same steps 1-13 in algorithm 1 are applied for descrambling process, where T is replaced by Bst_τ.

5 Experimental Results

The scope of this section is to present an experimental result of our proposed scheme. We use the following medical images with two different image sizes 512 × 512 and



(a)

(b)

(c)

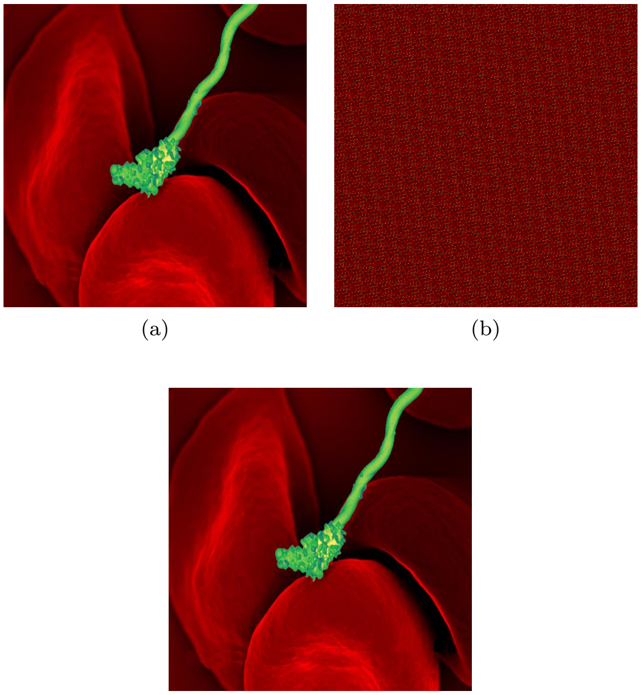
Figure 3: (a) MERS-CoV original image; (b) MERS-CoV encrypted image; (c) MERS-CoV decrypted image.

Algorithm 1: Arnold transformation scrambling algorithm Φ

```
Input: $Img_\rho$ // plain image
Output: $Img_\phi$ // encrypted image
$Img_\rho \leftarrow Img_\phi$
$T \leftarrow 1.4938N + 40.8689$ // Arnold transform
    period as in Equation (4)
$t \leftarrow 0$
$w \leftarrow Img_\rho.width$
$h \leftarrow Img_\rho.height$
while $t < T$ do
    for $i \leftarrow 0$ to $w$ do
        for $j \leftarrow 0$ to $h$ do
            $pixel \leftarrow Img_\rho[i][j]$
            $Img_\phi[(2*i+i) \bmod w][(i+j) \bmod h] \leftarrow$
            $pixel$
    $c[t] \leftarrow \sigma(Img_\rho, Img_\phi)$ // calculate the
        correlation coefficient
    $t \leftarrow t+1$
    return $Img_\phi$
for $m \leftarrow 0$ to $T-1$ do
    $count \leftarrow 0$
    for $n \leftarrow 0$ to $T-1$ do
        if $(c[m] < c[n])$ then
            $count \leftarrow count + 1$
    if $(count{=}T\text{-}1)$ then
        break
    $Bst_\tau \leftarrow m$ // Best iteration
```

Table 2: Experimental results of entropy analysis.

Image	Image status	Image size (KB)	entropy
Zika virus	Original 512 × 512	151.552	7.6145
	Encrypted 512 × 512	192.512	7.6072
	Decrypted 512 × 512	154.723	7.5904
	Original 256 × 256	40.960	7.5543
	Encrypted 256 × 256	49.783	7.5412
	Decrypted 256 × 256	42.152	7.5378
MERS-CoV	Original 512 × 512	163.840	7.7038
	Encrypted 512 × 512	200.704	7.6889
	Decrypted 512 × 512	178.254	7.6813
	Original 256 × 256	45.056	7.7016
	Encrypted 256 × 256	53.248	7.6946
	Decrypted 256 × 256	46.122	7.6865
TBRF	Original 512 × 512	73.728	7.9322
	Encrypted 512 × 512	143.360	7.8571
	Decrypted 512 × 512	96.364	7.7591
	Original 256 × 256	24.576	7.8814
	Encrypted 256 × 256	36.864	7.7802
	Decrypted 256 × 256	32.523	7.7791



(a) (b)

(c)

Figure 4: (a) TBRF original image; (b) TBRF encrypted image; (c) TBRF decrypted image.

256 × 256 24-bits:

1) Colorized image shows particles of Zika virus, which is a member of the family Flaviviridae. The virus particles are colored blue in the picture;

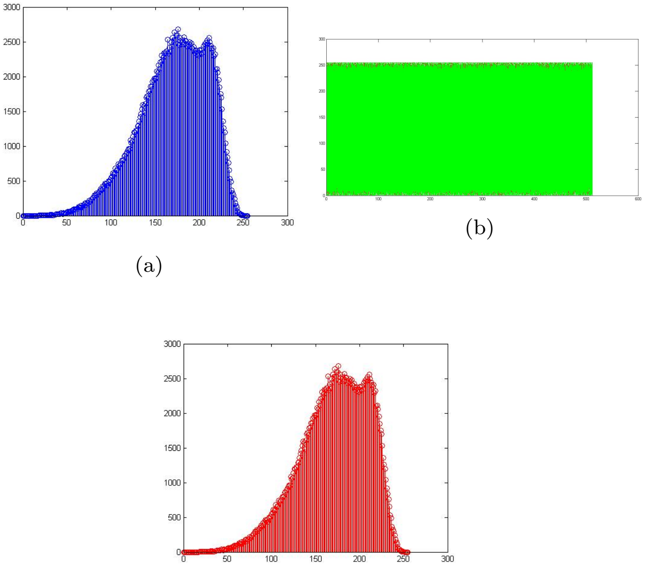
2) Colorized SEM showing numerous Middle East respiratory syndrome Coronavirus (MERS-CoV) viral particles (yellow) on the surface of a Vero E6 cell (blue);

3) Colorized SEM of a spiral-shaped Borrelia hermsii bacterium (green) on a number of red-colored red blood cells. B. hermsii is the causative agent of tick-borne relapsing fever (TBRF).

Figures 2, 3 and 4 show the above images and their corresponding encrypted and decrypted images respectively. Image encryption techniques aim to reduce the correlation of pixel positions and values until they are irrelevant to each other. Therefore, measurement tools used in this evaluation include entropy analysis and correlation coefficients. The entropy is given by Equation (5).

$$H(P) = -\sum_{i=1}^{n}\sum_{j=1}^{n} P(x_i, y_j)\log_2 P(x_i, y_j) \qquad (5)$$

where, $P(x_i, y_j)$ is the probability of pixel with coordinates (x_i, y_j) in original image appearing at the $[i^{th}][j^{th}]$ blocks in the scrambled image. As indicated in Table 2, the values of entropy analyses for all images are very close

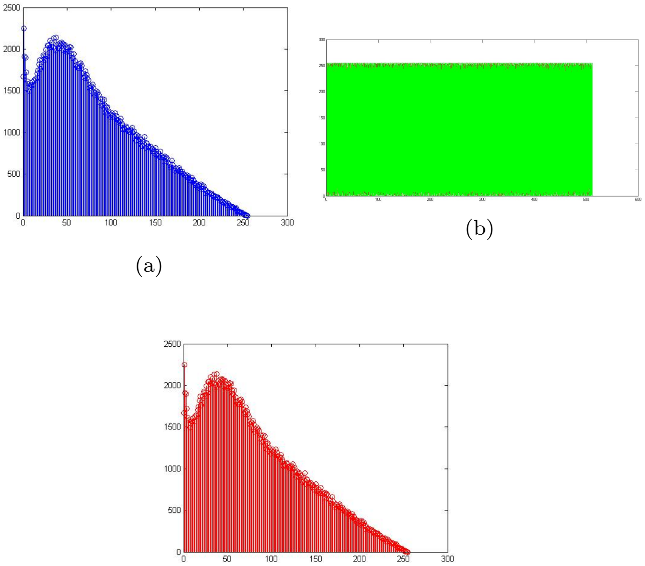


(b)

(a)

(c)

Figure 5: (a) Histogram of original Zika virus image ; (b) Histogram of encrypted Zika virus image; (c) Histogram of decrypted Zika virus image.



(b)

(a)

(c)

Figure 6: (a) Histogram of original MERS-CoV image ; (b) Histogram of encrypted MERS-CoV image; (c) Histogram of decrypted MERS-CoV image.

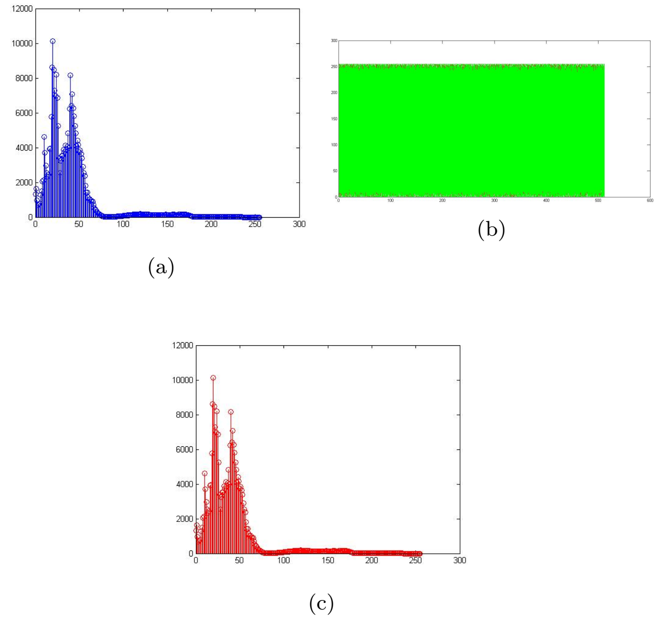


Figure 7: (a) Histogram of original TBRF image ; (b) Histogram of encrypted TBRF image; (c) Histogram of decrypted TBRF image.

to the ideal value 8 [7]. This confirms that the rate of information leakage is negligible in our scheme. Therefore, the proposed scheme successfully resists any kind of entropy attack.

Correlation coefficient means co-relation. It indicates the direction and degree (closeness) of linear relations between two variables X and Y. Correlation coefficient is denoted by ρXY or $\rho(X,Y)$, and is given by Equation (6).

$$\rho XY = \rho(X,Y) = \frac{Cov(X,Y)}{\sqrt{Var(X)Var(Y)}} = \frac{Cov(X,Y)}{\sigma_X \sigma_Y} \tag{6}$$

where Cov and Var are variance and covariance. Cov and Var are given by Equation (7) and Equation (8) respectively.

$$\begin{aligned} Cov(X,Y) &= E[(X-EX)(Y-EY)] \\ &= E[XY]-(EX)(EY) \end{aligned} \tag{7}$$

where E is statistical expectation.

$$Var(X) = E^2(X) - E(X^2) \tag{8}$$

As we adopt RGB images in this paper, the two-dimensional correlation coefficient r is employed [20, 27] to compare between original and encrypted images, r is given by equation

$$r = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{[i][j]}-\overline{A})(B_{[i][j]}-\overline{B})}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{[i][j]}-\overline{A})^2\sum_{i=1}^{M}\sum_{j=1}^{N}(B_{[i][j]}-\overline{B})^2}} \tag{9}$$

Table 3: Experimental results of correlation coefficients analysis

Image	Image size	Variance	Standard Deviation
Zika virus	512×512	$1.69271186518e^{-36}$	$1.3010e^{-18}$
	256×256	0	0
MERS-CoV	512×512	$7.52316384526e^{-37}$	$8.6736e^{-19}$
	256×256	$4.70197740329e^{-38}$	$2.1684e^{-19}$
TBRF	512×512	$6.56270479213e^{-35}$	$3.3212e^{-16}$
	256×256	$2.32221569203e^{-37}$	$4.6241e^{-18}$

where A is original (plain) image Img_ρ, B is encrypted (scrambled) image Img_ϕ. $A_{[i][j]}$ and $B_{[i][j]}$ are the intensity of the pixel in i^{th} row and j^{th} column for A and B respectively, and $\overline{A}$ is the mean of A and $\overline{B}$ is the mean of B. The values of the correlation coefficient satisfy the relation $-1 \geq r \geq 1$. N and M are the total numbers of pixel in each column and row respectively.

Table 3 shows the variance and standard deviation of correlation coefficients analysis. As seen in this table, the coefficient correlation between neighboring pixels are very close to the ideal value 0. This indicates that there is significant differences between the original image and its corresponding encrypted image according to the pixel coordinates.

5.1 Histogram Analysis

An image histogram is a graphical representation that shows the distribution of the intensity of pixels in a digital image. Statistical attack or histogram analysis attack repeat a series of histogram analysis to deduce the secret key or plain-pixels. Therefore, encrypted image should have a histogram with a uniform distribution. Figures 5, 6 and 7 show the histogram of the selected images: "Zika virus", "MERS-CoV" and "TBRF" respectively. Comparing the histograms of plain image with encrypted and decrypted images in each figure, it found that there is no resemblance between the histogram of original image and the histogram of encrypted image, while the histogram of original image is very similar to the histogram of decrypted image. Furthermore, the histograms of encrypted images are distributed uniformly. Hence, the proposed scheme is robust against histogram analysis attack.

6 Conclusion

In this paper, we have proposed a secure image encryption scheme for medical applications by incorporating the Arnold transformation and pairing-free identity-based authenticated key agreement protocol. After that, we have experimentally estimated the robustness and performance of our scheme. The analyses and results demonstrate that our scheme is efficient and secure. The long-term results of this effort is to offer a practical medical image watermarking that provides authentication and integrity control.

References

[1] D. Arroyo, C. Li, S. Li, G. Alvarez, and Wolfgang A. Halang, "Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm," *Chaos, Solitons & Fractals*, vol. 41, no. 5, pp. 2613–2616, 2009.

[2] M. Ashtiyani, P. M. Birgani, and H. M. Hosseini, "Chaos-based medical image encryption using symmetric cryptography," in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, pp. 1–5, April 2008.

[3] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences*, vol. 180, no. 15, pp. 2895–2903, 2010.

[4] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[5] J. Chen, J. Zhou, and K. W. Wong, "A modified chaos-based joint compression and encryption scheme," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 58, pp. 110–114, Feb 2011.

[6] L. J. Chen and A. D. Shen, "A novel public key image cryptosystem based on elliptic curve and arnold cat map," in *Advanced Materials Research*, vol. 989, pp. 4183–4186. Trans Tech Publ, 2014.

[7] W. B Chen and X. Zhang, "Image encryption algorithm based on henon chaotic system," in *2009 International Conference on Image Analysis and Signal Processing*, pp. 94–97, April 2009.

[8] R. Enayatifar, A. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a {DNA} sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.

[9] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 213– 220, 2008.

[10] K. Hamdnaalla, A. Wahaballa, and O. Wahballa, "Digital image confidentiality depends upon arnold transformation and rc4 algorithms," *International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS*, vol. 13, no. 04, pp. 6–17, 2013.

[11] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[12] X. Huang, "Image encryption algorithm using chaotic chebyshev generator," *Nonlinear Dynamics*, vol. 67, no. 4, pp. 2411–2417, 2011.

[13] B. Jana, "Dual image based reversible data hiding scheme using weighted matrix," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 6–19, 2016.

[14] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[15] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," *Image Vision Comput.*, vol. 27, pp. 1371–1381, August 2009.

[16] C. Li, Y. Liu, T. Xie, and Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 2083–2089, 2013.

[17] L. Liu, Z. Cao, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 1–5, 2016.

[18] S. V. Miller, "Use of elliptic curves in cryptography," in *Advances in CryptologyCRYPTO85 Proceedings*, pp. 417–426. Springer, 1985.

[19] N. Mohananthini and G. Yamuna, "A study of dwt-svd based multiple watermarking scheme for medical images," *International Journal of Network Security*, vol. 17, no. 5, pp. 558–568, 2015.

[20] A. M. Neto, A. C. Victorino, I. Fantoni, D. E. Zampieri, J. V. Ferreira, and D. A. Lima, "Image processing using pearson's correlation coefficient: Applications on autonomous robotics," in *Autonomous Robot Systems (Robotica), 2013 13th International Conference on*, pp. 1–6, April 2013.

[21] N.K. Pareek, Vinod Patidar, and K.K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926– 934, 2006.

[22] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, February 1978.

[23] M. A. Scholl, M. K. Stine, J. Hash, P Bowen, L. A. Johnson, C. D. Smith, and D. I. Steinberg. "Sp 800-66 rev. 1. an introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule,". tech. rep., Gaithersburg, MD, United States, 2008.

[24] Ercan Solak and Cahit okal, "Algebraic break of image ciphers based on discretized chaotic map lattices," *Information Sciences*, vol. 181, no. 1, pp. 227–233, 2011.

[25] F. Y. Sun and Z. W. Lu, "Digital image encryption with chaotic map lattices," *Chinese Physics B*, vol. 20, no. 4, p. 040506, 2011.

[26] X. Tong and M. Cui, "Image encryption scheme based on 3d baker with dynamical compound chaotic sequence cipher generator," *Signal Process.*, vol. 89, pp. 480–491, April 2009.

[27] V. Tsagaris and V. Anastassopoulos, "Multispectral image fusion for improved rgb representation based on perceptual attributes," *International Journal of Remote Sensing*, vol. 26, no. 15, p. 3241C3254, 2005.

[28] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, "Attacks on digital watermarks: Classification, estimation-based attacks, and benchmarks," *IEEE Communications Magazine*, vol. 39, pp. 118–126, 2001.

[29] A. Wahaballa, H. Xiong, F. Li, Z. Qin, and Z. Qin, "Secure mobile agent-based english auction protocol using identity-based signature scheme," *Int. J. Security and Networks*, vol. 11, no. 4, pp. 175–187, 2016.

[30] O. Wahballa, A. Wahaballa, F. Li, and C. Xu, "A secure and robust certificateless public key steganography based on svd-ddwt," *International Journal of Network Security*, vol. 18, no. 5, pp. 888–899, 2016.

[31] X. Zhang, G. Zhu, W. Wang, M. Wang, and S. Ma, "Period law of discrete two-dimensional arnold transformation," in *Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on*, pp. 565–569, Aug 2010.

[32] G. Zhao, X. Yang, B. Zhou, and W. Wei, "RSA-based digital image encryption algorithm in wireless sensor networks," in *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*, vol. 2, pp. V2–640–V2–643, July 2010.

[33] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29–37, 2012.

[34] Z. L. Zhu, W. Zhang, K. W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

Biography

Osman Wahballa received the B.S. degree in electrical engineering and computer engineering from Karary University, Department of Electrical Engineering in 2006, Khartoum, Sudan, and the M.S. degree in M.Sc. in Computer Engineering, Information Security form University of Electronic Science and Technology of China in 2013, Chengdu, China. He is currently working toward the Ph.D. degree in computer science from University of Electronic Science and Technology of China. His current research interests include information hiding, steganography, and cryptography.

Abubaker Wahaballa is currently working as a Postdoctoral Fellow at School of Information and Software Engineering, University of Electronic Science and Technology of China UESTC. He received his PhD degree from UESTC in 2015. His current research interests include information security, cryptography, steganography, and DevOps.

Fagen Li Fagen Li received his Ph.D. degree in cryptography from Xidian University, Xian, China in 2007. He is now an associate professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. His recent research interests include cryptography and network security. He has published more than 70 papers in the international journals and conferences.

Idris Ibn idris earned his BEng degree in Electrical Engineering at Ahmadu Bello University, Zaria, Nigeria in 2008 and MSc degree in Applied Instrumentation and Control at Glasgow Caledonian University, Scotland, United Kingdom in 2011. He is currently pursuing the PhD degree in Power Systems and Automation with the School of Electric Power, South China University of Technology, Guangzhou, China. His current research interests include Instruments Communication and Networking, Power Systems Operations and Control, and Information Security.

Chunxiang Xu received her B.Sc., M.Sc. and Ph.D. degrees at Xidian University, in 1985, 1988 and 2004 respectively, P.R. China. She is presently engaged in information security, cloud computing security and cryptography as a professor at University of Electronic Science Technology of China (UESTC).