A Secure and Robust Certificateless Public Key Steganography Based on SVD-DDWT

Osman Wahballa, Abubaker Wahaballa, Fagen Li and Chunxiang Xu
(Corresponding author: Abubaker Wahaballa)

School of Computer Science and Engineering, University of Electronic Science and Technology of China
No.4, Section 2, North Jianshe Road, Chengdu, P.R. China
(Email: wahaballah@hotmail.com)
(Received July 15, 2015; revised and accepted Sept. 29 & Nov. 2, 2015)

Abstract

Security and undetectability are main goals of steganographic systems. This paper proposes a novel certificateless public key steganography that allows two parties that have no prior knowledge of each other to communicate covertly over public channel. Firstly, secure and high efficient rate of key distribution are provided. Secondly, proper stego and destego are introduced based on Distributed Discrete Wavelet Transform (DDWT) and Singular Value Decomposition (SVD).Thirdly, we present the Matlab analysis of the original and stego images, which proves the robustness of our scheme. Finally, the analyses demonstrate that our scheme meets all security requirements of steganographic system and resists various kinds of sophisticated attacks.

Keywords: Certificateless public key steganography, distributed discrete wavelet transform, singular value decomposition

1 Introduction

While cryptography is about enciphering the content of messages in secret code or cipher, steganography aims to transmit the content of messages inside a perfectly innocent covers. Steganography [13] is a skill of concealing communication between two parties in the presence of third party called adversary. The term derived from Greek, literally means hidden writing. It includes many different forms of secret communication techniques that hide a secret message within *cover-text* so that others cannot see or know of any hidden message. These techniques have evolved from a simple and primitive techniques, such as invisible inks and microdots to other, more complex and sophisticated, such as covert channels, spread spectrum, and transformation domain techniques.

In order to safeguard information and communication between sender and receiver, and to stave off an attacker from breach of sensitive information, a steganographic message will appear to be something else as shown in Figure 1. It can be: plain text, image, an audio, video or TCP/IP [25].

Current public key steganography schemes have been constructed based on traditional public-key infrastructure (PKI) or Identity-based cryptosystem (IBC). However, PKI-based schemes are adversely affected by the complex procedures of certificates management and verification, while the obvious drawback of IBC is an escrow problem.

With a view to solve the key escrow problem in identity-based public key cryptosystem (ID-PKC) [7], Al-Riyami and Paterson [3] proposed a certificateless public key cryptosystem (CL-PKC) which contains the attractive features of ID-PKC (certificateless property). Furthermore, the reliance on trusted third party is much reduced. Wang *et al.* [26] and Baek *et al.* [6], both made their marks to list the features of CL-PKC which include:

- CL-PCK facilitates the complex certificate management process in the traditional public key cryptography;
- The key generation center (KGC) in CL-PKC is incapable to generate the user's whole private key, which does not have the highest priority for key generation.
- CL-PCK provides lower computational costs and communication overheads.

Finally, we remark that CL-PKC provides several useful and appealing features. Therefore, we take advantage of these features to construct a secure and robust certificateless public key steganography scheme.

1.1 Motivations

The *Prisoner's Problem* [21] is considered as the motivation of this paper. In this problem, Alice and Bob are in prison, and are considering a means to escape but the only way they can relay information to and from each other is via a public channel under the hearing and eyesight of

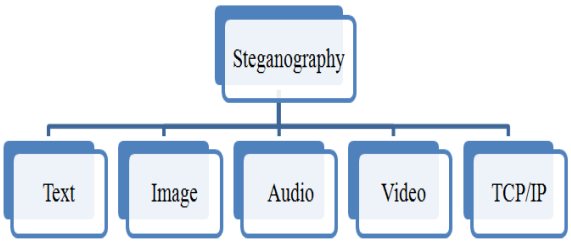

Figure 1: Types of steganography

a warden, Wendy. With a view to avoid Wendy's suspicion, they have to communicate as invisible as possible so that they will not be revealed by Wendy. Invisibility is an essential point in steganographic systems. Furthermore, the efficient key management of CL-PKC is useful for public key steganographic systems, especially when the Key Generation Center (KGC) is incapable to hold the user's whole private key, which does not have the full power for key generation. It just generates a user's partial private key from the user's identity. That is why certificates are no longer needed in CL-PKC.

Our contributions are the following folds:

1) A novel public key certificateless steganography is proposed;
2) Highly efficient rate for key distribution and management is provided;
3) The key escrow problem is addressed.
4) Proper *Stego* and *Destego* are offered.

1.2 Security Issues in Steganographic Systems

In general, a practical and secure steganographic system should satisfy the following requirements:

- ***Robustness***: The embedded data must be kept intact if the stego-system undergoes transformation, such as spatial domain and frequency domain transformation; linear and non-linear filtering; addition of random noise etc.
- ***Undetectability***: The hidden text (steganographic message) should appear identical to all possible statistical tests which can be carried out.
- ***Indistinguishability***: It means that it is hard to distinguish between covertext and stegotext.
- ***Security***: It is said that the embedded algorithm is secure if the hidden-data is not subject to removal after being discovered by the attacker.

The paper is organized as follows. Related works and pervious result are discussed in Section 2. In section 3, we briefly introduce the preliminaries used in this paper. A novel certificateless steganography is proposed in section 4. Section 5 deals with efficiency comparison and security analysis. The experimental results are presented in Section 6. Finally, conclusion and recommendation for future works are given in Section 7.

2 Related Works

Public key steganography was first considered by Anderson [4]. However, only informal security model was proposed. In 2002, Guillon *et al.* [9] introduced an experimental study for steganalysis of scalar costa scheme (SCS). This scheme was applied to PCM audio contents. It was designed based classical public-key cryptosystem that is RSA. The disadvantages of RSA are: i) Very slow key generation; ii) Two-part key is vulnerable to GCD attack if poorly implemented. In 2004, the basic notations of steganographic security against adaptive chosen-covertext attacks (SS-CCA) and steganographic security against publicly-detectable replayable adaptive chosen-covertext attacks (SS-PDR-CCA) was defined formally by Backes and Cachin [5] in IBM laboratory at Zurich. Ahn and Hopper [2] introduced the first protocols for public-key steganography and steganographic key exchange in random oracle model. Le and Kurosawa [14, 15, 16] proposed serial versions of stegosystem. However, these schemes are not in line with the standard model of chosen hiddentext attacks. Hopper and Ahn [12] proposed a provably secure steganography scheme based on unbiased functions. However, this scheme had extremely low information rates. Ahadpour *et al.* [1] proposed a method for the public key steganography based on Discrete Cross-Coupled Chaotic Maps. This method was used to specify the location of the different parts of the secret data in the JPEG image. Ahadpour's method was based on the diffie-hellman key exchange algorithm. However, there are some drawbacks in this algorithm that are discrete logarithm and Man-in-the-Middle attack. Recently, Ruffing *et al.* [19] introduced the concept of *Identity-Based Steganography*. However, the key escrow problem in this scheme is not a good property for public key steganographic systems.

In this paper, an efficient certificateless public key steganography scheme is proposed. Our model does not only satisfy the security requirements of steganographic systems, but it is also able to improve the computational costs and communication overheads.

3 Preliminaries

In this section, we give a brief introduction on the preliminaries required in this paper which include computational hardness assumptions, discrete wavelet transform and singular-value decomposition (SVD).

3.1 Computational Hardness Assumption

Our scheme is based on the hardness assumptions as follows:

1) Discrete Logarithm (DL) Problem: Given a generator P of a cyclic group $\mathbb{G}^*$ with order q, and $x \in \mathbb{Z}_q^*$ satisfying $Q = xP$.

2) Divisible computational DiffieHellman (DCDH) problem: Given (aP,bP) then compute $ab^{-1}P$, where $P \in \mathbb{G}$ is the generator and $a, b \in \mathbb{Z}_q^*$ is unknown.

3.2 Discrete Wavelet Transform

In the last few decades, Discrete Wavelet Transform (DWT) [8, 20] had been adopted and deployed in an extensive range of applications including numerical analysis, signal analysis, pattern recognition, computer vision, image/video coding, steganography and watermarking. Wavelet transform provides both time and frequency information simultaneously. In this transform, time domain is passed through low-pass and high-pass filters (band-pass) to get low and high frequencies respectively. The advantage of DWT is that provided a better compression ratio without losing more information of image.

Discrete wavelet transform has several types. The oldest and most known one is the Haar DWT [22] which includes two steps, namely the horizontal process and vertical process. The neighboring pixies is used to perform the horizontal process from left to right then execute the vertical process from top to bottom as shown in Figure 5. The LL sub-band is used to embed the steganographic message (secret message). However, this sub-band is vulnerable to the image cropping attacks. In order to address this problem, Lin *et al.* [17] suggested Distributed Discrete Wavelet Transform (DDWT). In this method, multi-scale DDWT is used to transform the image data from spatial domain into frequency domain and then hide the steganographic message in the frequency domain and perform inverse multi-scale DDWT transformation (IDDWT) to get stego image in spatial domain. The steganographic method in this paper is based on Lin's Distributed Discrete Wavelet Transform (DDWT).

3.3 Singular-Value Decomposition

Singular-Value-Decomposition (SVD) is a useful tool for matrix factorization [23]. For any digital image A of size $m \times n$ with $m \geq n$, can be represented by A's SVD as follows:

$$A = U\Sigma V^T = \sum_{i}^{m} \sigma_i u_i v_i^T \quad (1)$$

where $U_{m\times t}$ and $V_{n\times t}$ are orthogonal matrices and $\Sigma_{t\times t}$ is a diagonal matrix representing the singular values on

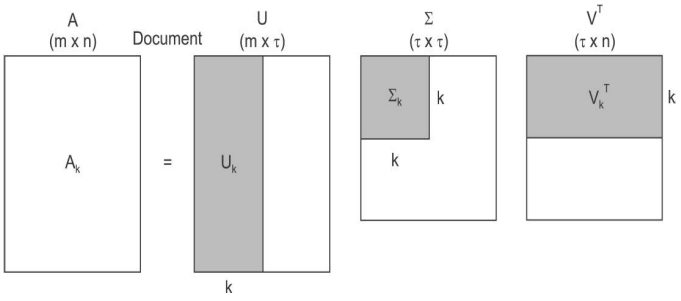

Figure 2: SVD decomposition

top of $m - n$ rows of zeros:

$$\Sigma = \begin{bmatrix} \sigma_1 & & & & 0 \\ & \sigma_2 & & & \\ & & .. & & \\ & & & .. & \\ 0 & & & & \sigma_m \end{bmatrix}$$

The columns of matrix U are the left singular vectors (eigenvectors U_k) and V^T has rows that are the right singular vectors (eigenvectors V_k). As shown in Figure 2, calculating the SVD consists of finding the eigenvectors and eigenvalues of U_k and V_k^T.

4 Proposed Model

In this section a novel public key certificateless steganography is proposed. The notations of our proposed model used in this paper are shown in Table 1. The KGC is adopted as a key generation center. Our proposed model is expressed diagrammatically in Figure 3. Alice and Bob are in prison, and want to relay information to and from each other is via a public channel under the watch of a warden, Wendy. To avoid Wendy's censorship, Alice sends to Bob some innocuous contents. Alice is said to be active when she embeds a hidden message h_{txt} modifying the cover-text C_{txt} into stego-text S_{txt}. Alice is not active when she sends really innocuous contents.

In order to establish a secure communication channel between Alice and Bob, we describe the eight algorithms needed to define our scheme based on Alriyami and Paterson [3] and He *et al.* [10] schemes, which include: `Setup`, `Set Secret Value`, `Partial Private Key Extract`, `Set Private key`, `Set Public Key`, `Key-Agreement`, `Stego` and `Destego`.

1) `Setup`: Initially, the KGC inputs the security parameters. These include the tuple $\{F_q, E|F_q, G, P\}$ as defined in Section 3. The KGC randomly chooses its master-key $s \in \mathbb{Z}_n^*$ and computes its public master-key $P_{pub} = sP$, and chooses two hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_n$ and $H_2 : \{0,1\}^* \to \mathbb{Z}_n$.

   Finally, the KGC publishes the system parameters: $params = (F_q, E|F_q, G, P, P_{pub}, H_1, H_2)$.

2) `Set Secret Value`: Alice A with identity ID_A selects $x_A \in \mathbb{Z}_n^*$ and sets x_A as secret value.

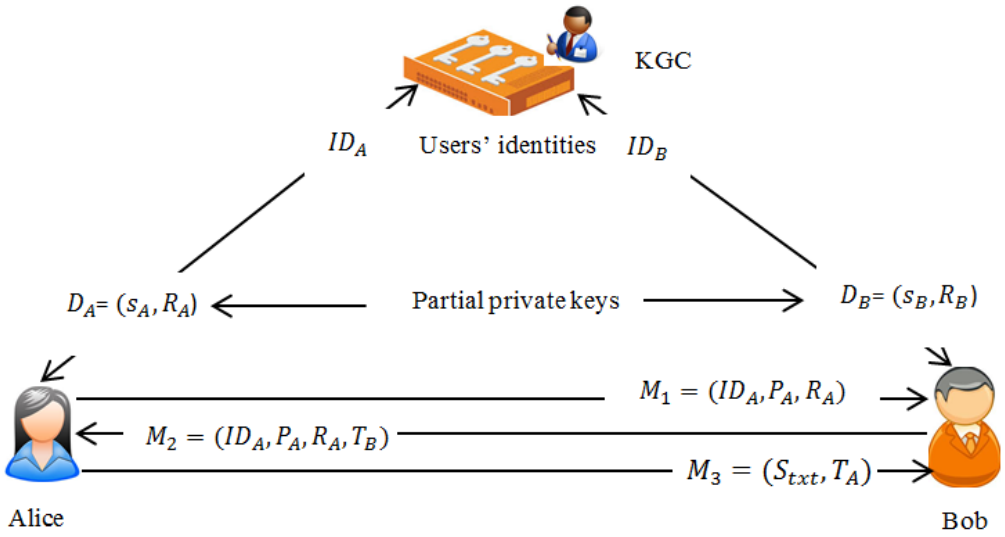

Figure 3: Proposed model

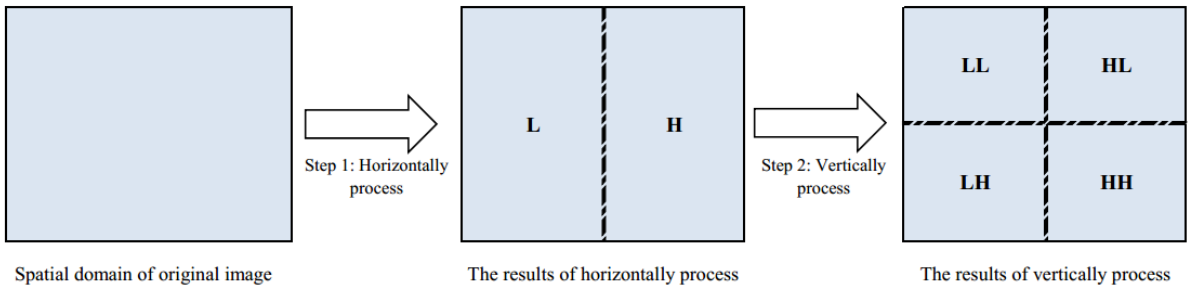

Figure 4: 1-scale DDWT

3) `Partial Private Key Extract`: KGC computes the partial private key of Alice with identity ID_A as follows:
   - KGC chooses $r_A \in \mathbb{Z}_n^*$, computes: $R_A = r_A P$ and $h_A = H_1(ID_A, R_A)$;
   - Then, KGC computes $s_A = r_A + h_A s \bmod n$;
   - KGC sets the tuple $D_A = (s_A, R_A)$ as partial private key.
   - KGC sends D_A secretly to Alice.

4) `Set Private key`: When Alice receives D_A from the KGC, Alice can validate the partial private key by checking whether the equation $s_A P = R_A + h_A P_{pub}$ holds. If it holds, then Alice sets the pair $S_A = (x_A, D_A)$ as her full private key.

5) `Set Public Key`: Alice computes her public key as $P_A = x_A P$:

   Bob with identity ID_B can repeat algorithms from 2 to 5 to generate his keys.

6) `Key-Agreement`: The common authenticated per session secret key can be computed at both sides as follow:
   - Alice sends $M_1 = (ID_A, R_A, P_A)$ to Bob;
   - Upon Bob receiving M_1, he chooses at random the ephemeral key $b \in \mathbb{Z}_n^*$ and computes $T_B = b(P_A + R_A + H_1(ID_A, R_A)P_{pub})$. Then, Bob sends $M_2 = (ID_B, R_B, P_B, T_B)$ to Alice;
   - After receiving M_2, Alice chooses at random the ephemeral key $a \in \mathbb{Z}_n^*$ and computes $T_A = a(P_B + R_B + H_1(ID_B, R_B)P_{pub})$. Then, Alice sends $M_3 = (T_A)$ to Bob;
   - Then, both sides can compute the shared secrets as follows:
     - Alice computes $K_{AB}^1 = (x_A + s_A)^{-1} T_B + aP$ and $K_{AB}^2 = a(x_A + s_A)^{-1} T_B$;
     - Bob computes $K_{BA}^1 = (x_B + s_B)^{-1} T_A + bP$ and $K_{BA}^2 = b(x_B + s_B)^{-1} T_A$.
   - Eventually, Alice and Bob can compute the shared secret keys as:

$$\begin{aligned} sk &= H_2(ID_A||ID_B||T_A||T_B||K_{AB}^1||K_{AB}^2) \\ &= H_2(ID_A||ID_B||T_A||T_B||K_{BA}^1||K_{BA}^2). \end{aligned}$$

7) `Stego`: If Alice want to send secret message h_{txt} (hidden message) to Bob into cover-content C_{txt}, she can execute the following algorithm:

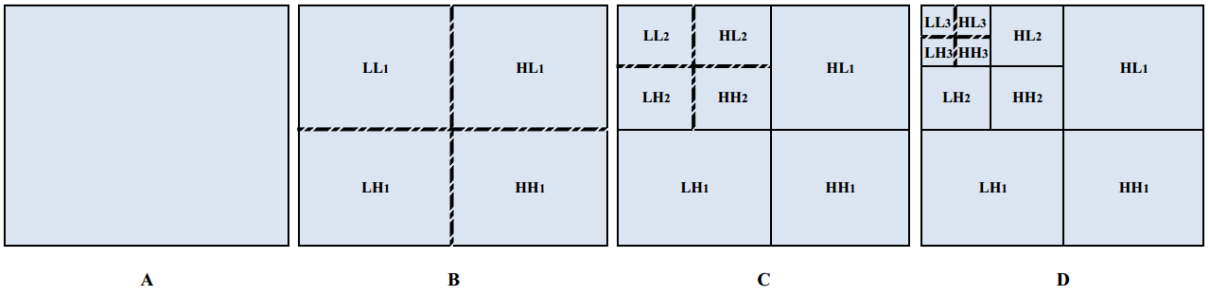

Figure 5: Multi-scale DDWT transforms: (A) The original image (B) 1-scale DDWT (C) 2-scale DDWT (D) 3-scale DDWT

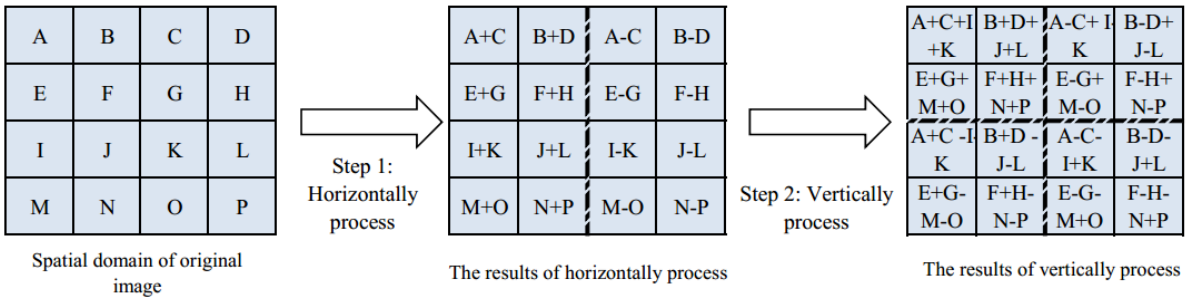

Figure 6: 1-scale DDWT: Horizontal and vertical processes on an original image with 4×4 dimensions

- Alice embeds a secret message h_{txt} into stego-content S_{txt} by modifying the cover-content C_{txt} as: $S_{txt} = \varepsilon_{sk}(h_{txt}, C_{txt})$, where ε is the embedding algorithm;
- Then, Alice sends the S_{txt} to Bob.

8) `Destego`: Bob destegos Alice's hidden message with shared key as follows: $< h_{txt}, C_{txt} >= \beta_{sk}(S_{txt})$.

4.1 Steganographic Method

The steganographic method in this paper is based on Lin's et al DDWT, which consists of two steps: horizontal process and vertical process. The details of these processes are described as follows.

4.1.1 Horizontal Process

In this process, the original image is separated horizontally into two equal blocks. Then, from left to right add and subtract corresponding pixels on the two sub-blocks. At the end of this process, the pixels on the left sub-block are replaced with result of addition, while the result of the subtraction replaces the pixels on the right sub-block. The left sub-block represents the low frequency domain and is denoted as L; the right sub-block represents the high frequency domain and is denoted as H.

4.1.2 Vertical Process

From the blocks generated by the horizontal process above, the image is separated vertically into equal sub-blocks. Then, from upper to lower add and subtract corresponding pixels on the two sub-blocks. The pixels on the upper sub-block are replaced with result of addition, while the result of the subtraction replaces the pixels on the lower sub-block. Thus, four sub-blocks are generated and denoted as LL, LH, HL and HH. Figure 4 shows these sub-blocks. The Step-1(horizontal process) and Step-2 (vertical process) are repeated 2 k times. Figure 5 shows the k-scale DDWT transform, while 1-scale DDWT: horizontal and vertical processes on an original image with 4×4 pixels is shown in Figure 6.

As indicated in embedding algorithm ε, we set input, output and the algorithm parameters in Steps 1-3. Steps 4-10 show the decomposition process (multi-scale DDWT) for the coverImg. Then, we perform SVD for diagonalImg blocks. Steps 12-16 show the embedding process. Finally, we apply inverse DDWT for srego-blocks to obtain the stego-image.

As shown in Extract Algorithm β, from Steps 1-3 we set the input, output, and the parameters. Then, we perform DDWT for stegoImg in Steps 4-9. The SVD process is applied in Step 10, while we extract the secret message Msg in Steps 11-15.

5 Efficiency Comparison and Security Analysis

The security and efficiency of the proposed scheme is analyzed in this section. Security requirements of our proposed model are discussed in Section 5.1, while efficiency

Algorithm 1: Embedding algorithm ε

Input: $coverImg, Msg$
Output: $stegoImg$

$Bit \leftarrow M_0, M_1, .., M_{65535}$ // Extract Bit set of Msg
$w \leftarrow coverImg.width$
$h \leftarrow coverImg.height$
// Decomposition process
for $i \leftarrow w$ ***downto*** 0 **do**
  for $j \leftarrow h$ ***downto*** 0 **do**
    $w \leftarrow (w+1)/2$
    $h \leftarrow (h+1)/2$
    $HorizontalImg^{LLLH} \leftarrow coverImg(w,h)$
    $VerticalImg^{HLHH} \leftarrow coverImg(w,h)$
    $diagonalImg^{LHHL} \leftarrow coverImg(w,h)$
    $[U,S,V] \leftarrow SVD(diagonalImg^{LHHL})$
      // Perform SVD for diagonalImg blocks
  for $k \leftarrow 1$ ***to*** $Msg.length$ **do**
    if $M_k = 0$ **then**
      $HorizontalImg_{ij}^{LL} \leftarrow M_k$
      else
        $VerticalImg_{ij}^{HH} \leftarrow M_k$
$stegoImg \leftarrow IDDWT(stego\_blocks)$// Apply Inverse DDWT for srego_blocks to obtain the stego-image
return $stegoImg$

Algorithm 2: Extract algorithm β

Input: $stegoImg$
Output: Msg

$Bit \leftarrow M_0, M_1, .., M_{65535}$ // Bit set of Msg
$w \leftarrow StegoImg.width$
$h \leftarrow StegoImg.height$
for $i \leftarrow w$ ***downto*** 0 **do**
  for $j \leftarrow h$ ***downto*** 0 **do**
    $w \leftarrow (w+1)/2$
    $h \leftarrow (h+1)/2$
    $StegoImg^{LLLH} = StegoImg(w,h)$
    $StegoImg^{HLHH} = StegoImg(w,h)$
    $[U,S,V] \leftarrow SVD(stegoImg^{LHHL})$
      // Perform SVD for diagonalImg blocks
  if $StegoImg_{ij}^{LLHH} < 0$ **then**
    $M_i = 0$;
    else
      $M_i = 1$;
  $Msg = Combine(M_i)$
return Msg

Table 1: Notations of our proposed model

Notation	Meaning
KGC	A key generation center
ID_A	Alice's A's Identity
ID_B	Bob's B's Identity
P_A	Alice's public key
P_B	Bob's public key
P_{pub}	The KGC's master key
X_A	Alice's secret value
X_B	Bob's secret value
S_A	Alice's private key
S_B	Bob's private key
D_A	Alice's partial private key
D_B	Bob's partial private key
sk	Shared secret key
h_{txt}	A hidden text (steganographic message)
C_{txt}	A cover content
S_{txt}	Stego content
H_1, H_2	Two hash functions
ε	Embedding algorithm (steganography algorithm)
β	Extract algorithm

comparison is presented in Section 5.3.

5.1 Correctness

It can be easily seen that $K_{AB}^1 = K_{BA}^1$ and $K_{AB}^2 = K_{BA}^2$. Hence, the shared secrets are agreed.

$$\begin{aligned} K_{AB}^1 &= (x_A + s_A)^{-1} T_B + aP \\ &= bP + aP \\ K_{BA}^1 &= (x_B + s_B)^{-1} T_A + bP \\ &= aP + bP \\ K_{AB}^2 &= a(x_A + s_A)^{-1} T_B \\ &= abP \\ K_{BA}^2 &= b(x_B + s_B)^{-1} T_A \\ &= baP. \end{aligned}$$

5.2 Security

As proved in [10], our protocol satisfies all security requirements of authenticated key agreement:

- *Known-key secrecy*: It allows to run the key exchange protocol several times. In each time, Alice and Bob should obtain a unique session key which depends on

Table 2: Efficiency comparison

Steganographic Model	Computational Costs			Message Exchange
	T_{mul}	T_H	T_e	
Ruffing *et al.* [19]	2	4	2	2
Our model	8	5	0	3

every particular ephemeral key $a, b \in \mathbb{Z}_n^*$ for Alice and Bob receptively. Even if the adversary $\mathcal{A}$ has learned some other session keys, s/he cannot compute the keying point $E_q(a, b)$ from aP and bP. because when s/he has no access to a and b, s/he faces the Divisible computational Diffie-Hellman (DCDH) problem which is believed to have no polynomial time algorithm to compute. Hence, the known-key security property is achieved in our protocol.

- *Forward secrecy*: Compromising the long-term private keys of Alice and Bob will not reveal previously established session keys. It is obvious that the adversary $\mathcal{A}$ cannot compute T_A and T_B without knowing of R_A and R_B even with providing the long-term private keys of Alice and Bob. So, our protocol has perfect forward secrecy.

- *Key-compromise impersonation*: Suppose that an adversary $\mathcal{A}_{\mathcal{I}}$ has replaced Bob's public key with $P_B = x_e P$, where $x_e \in \mathbb{Z}_n^*$ is selected by himself, he could not compute the T_B or T_A without knowing of ephemeral short private keys a, b. Then, considering type II adversary, $\mathcal{A}_{\mathcal{II}}$ has known the KGC's master key s and Bob's partial key D_B, but he cannot generate $K_{AB}^1, K_{BA}^1, K_{AB}^2$ or K_{BA}^2 without knowing the values of ephemeral short private keys a, b and long-term private keys x_A and x_B of Alice and Bob, since he also cannot solve the (DCDH) problem.

- *Unknown key-share resilience*: Suppose an adversary $\mathcal{A}$ attempts to coerce Alice to share a session key with him, while Alice believes a session key is shared with Bob. For $\mathcal{A}$ to launch this attack successfully, he should force Alice and Bob to share the same secret. However, our protocol including the identities information of participating peers in computing the session key can prevent UKSR attack.

5.3 Efficiency Comparison

In this section, the comparison of our model against Ruffing *et al.* [19] is presented, the computational costs and communication overheads are highlighted in Table 2. For convenience, we define the following notations: T_H(the time complexity of one-way hash function); T_e(the time complexity of pairing operation); T_{mul}(the time complexity of a scalar multiplication operation of point).

As indicated in Table 2, Ruffing *et al.* [19] model requires two times bilinear pairing operation in session key agreement. However, a bilinear pairing operation is more time-consuming than other operations [7]. Its relative computation cost is approximately twenty times higher than that of the scalar multiplication over elliptic curve group [11]. Furthermore, the key escrow problem is addressed in our model. In other words, in our model the KGC cannot impersonate the user without being detected, while this feature is lacking in Ruffing *et al.* [19].

6 Experimental Results

We have conducted a series of repeated experiments using 512 × 512 24-bits standard RGB images: "Lena", "Baboon", "Peppers", "Jet" and "Barbara". The embedding capacity is measured in terms of bits. Steganographic method of this paper is implemented using Java 8 in environment as follows: HP-Compaq 610 laptop computer with Intel ® Core(TM)2 Duo CPU T5870 2.00GHz (2CPUs), 2.00 GHz, Memory RAM 1024MB, running on Windows 7 32-bit operating system. For evaluation test, we use Matlab R2013a 8.1.

The measurement tools used in this evaluation include Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). MSE and PSNR are mostly used for evaluating the robustness of steganographic system. The mean-squared error (MSE) between two images $A = \{a_1..a_M\}$ and $A' = \{a'_1..a'_M\}$ is given by Equation (2), where M is the number of pixels.

$$MES(A, A') = 1/M \sum_{i}^{m} (a_i - a'_i)^2 \tag{2}$$

PSNR is the ratio between the original signal and the stego signal in the image given in decibels. Formula (3) shows the PSNR test. For images $A = \{a_1..a_M\}$ and $A' = \{a'_1..a'_M\}$, and MAX equal to the maximum possible pixel value ($2^8 - 1 = 255$ for 8-bit image).

$$PSNR = 10 \log_{10}(\frac{MAX^2}{MSE(A, A')}) \tag{3}$$

As seen in Equations 2 and 3, there is an inverse relationship between MSE and PSNR, a low value of MSE give rise to higher value of PSNR, which signifies that a higher value of PSNR shows the higher quality of the image.

As indicated in Table 3, the average of PSNR values is 53.66 db, while MSE average is 0.48. This confirms that the proposed steganographic method is good in terms of invisibility of the embedded data. In other words, it is

Table 3: Experimental results of original and stego image

Image	Hiding capacity (bits)	PSNR	MSE
Lena	3,547,174	55.67	0.18
baboon	2,822,323	56.39	0.15
peppers	4,272,027	55.03	0.20
Jet	2,336,136	45.86	1.69
Barbara	3,909,601	55.34	0.19
Avg.	3,377,452	53.66	0.48

Table 4: Experimental results in the presence of Gaussian filter

Image	σ	MSE	PSNR
Baboon	0.1	0.1492602	56.391363
	0.2	0.1492602	56.391363
	0.25	0.1492602	56.391363
	0.27	0.1493619	56.388404

hard to distinguish between covertext and stegotext. Also graphical comparisons are presented in Figures 7, 8 and 9 for original and stego images and Figures 10, 11 and 12 for original and stego histograms.

In the following, the results of evaluating the robustness of proposed steganographic method against various kinds of sophisticated attacks are presented.

6.1 Gaussian Filtering

Robustness of proposed steganographic method is evaluated against Gaussian filtering attack with window size of 5×5. Table 4 presents the mean squared error (MSE) and peak signal-to-noise ratio (PSNR) in the presence of Gaussian filter with window size of 5×5 and variance (sigma σ) between 0.1 and 0.3 for Baboon stego image. As indicated in Table 4, the Gaussian filtering attack does not affect the robustness of hidden text h_{txt} by a considerable amount. The proposed steganographic method does not fail under Gaussian filter with window size 5×5 and variance $\sigma \leq 0.27$.

6.2 Bilinear Interpolation Image Rescaling

The results of rescaling raw image data using bilinear interpolation of proposed steganographic method are presented in Table 5. We have shown that the hidden text h_{txt} have not been affected by rescaling the stego image. Figure 13 shows the result of this operation using two different compression ratios.

Figure 7: Original and stego Lena from left to right respectively

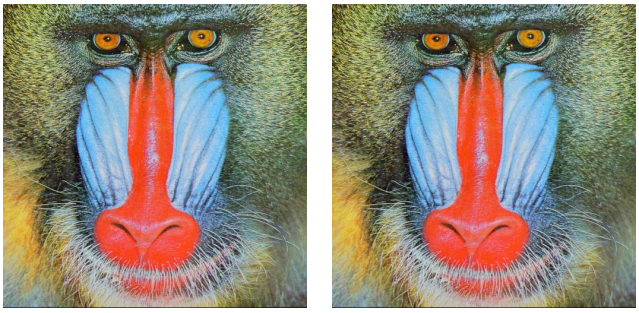

Figure 8: Original and stego Baboon from left to right respectively

Figure 9: Original and stego Peppers from left to right respectively

Table 5: Experimental results in the presence of Gaussian filter

Image	Compression ratio	MSE	PSNR
Lena	66%	0.176223	55.670159
	150%	0.176223	55.670159

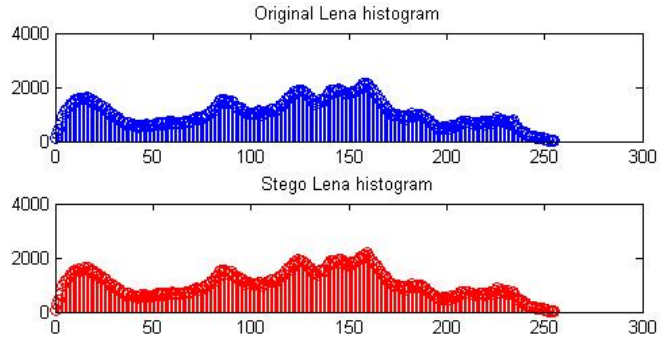

Figure 10: Original and stego Lena histograms

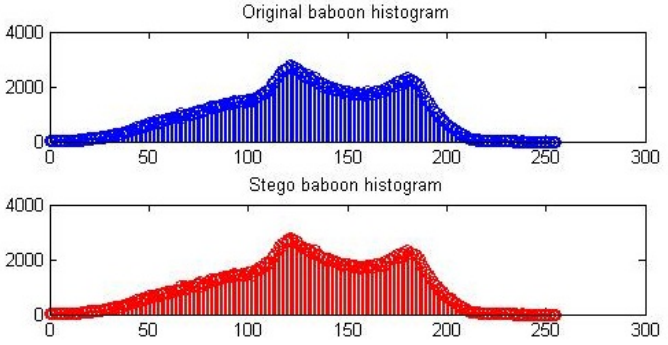

Figure 11: Original and stego Baboon histograms

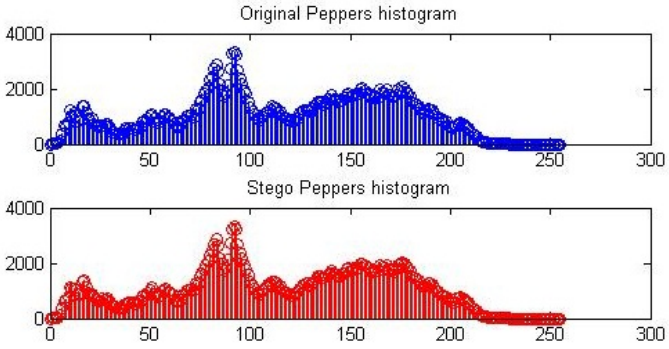

Figure 12: Original and stego peppers histograms

Figure 13: Rescaled image, bilinear interpolation, 66% and 150%' from left to right respectively

6.3 Pepper-Salt Noise Attack

Pepper-Salt noise causes on and off pixels. The results of evaluation of proposed steganographic method in the presence of Pepper-Salt noise are presented in Table 6. We adopted noise density between 0.000001 and 0.000005. As shown in Table 6, our steganographic method does not fail under Pepper-Salt noise with noise density ≤ 0.000005.

6.4 Pixel Difference Histogram Analysis

The results of difference histogram analysis are shown in Figure 14. From the figure, we observe that there are more numbers of bins which are close to 0 as compared to bins which are away from 0. Furthermore, the step pattern is not shown in the figure. Hence, the proposed steganographic method is robust against histogram analysis attack.

Table 6: Experimental results in the presence of pepper-salt noise

Image	noise density	MSE	PSNR
Baboon	0.000001	0.190282	55.336822
	0.0000015	0.190282	55.336822
	0.000005	0.298773	53.377383

6.5 Chi-Square Analysis

Chi-Square (χ^2) is a statistical test commonly used to calculate the average LSB and construct a table of frequencies and Pair of Values. Figure 15 shows the results of chi-square analysis on Baboon stego image. As the graph obtained fulfills the required range. Therefore, the proposed scheme successfully sustains this attack.

6.6 RS Analysis

RS analysis is one of the most reliable steganalysis which performs statistical analysis of the pixels to successfully detect the hidden message in an image. Figure 16 shows the results of RS analysis. From figure, we show that the difference between the relative number of regular groups (Non-overlapping groups) and the relative numbers of singular groups (Overlapping groups)is very small. The rule $R_M \cong R_{-M}$ and $S_M \cong S_{-M}$ are satisfied for Baboon stego image. This confirms that the proposed steganographic method is secure against RS attack.

6.7 Requirements Analysis and Comparison

Considering the importance and necessity of the security requirements of steganographic system that have been discussed in Section 1.2, we outline in this section how these requirements can be achieved using our proposed scheme.

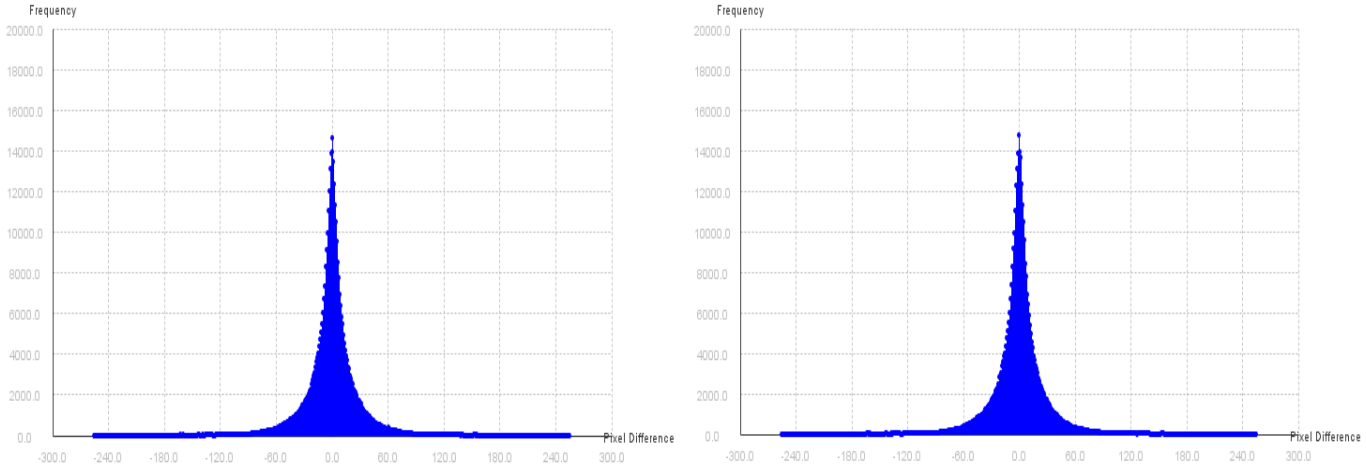

Figure 14: Pixel difference histogram analysis on baboon original and stego image from left to right respectively

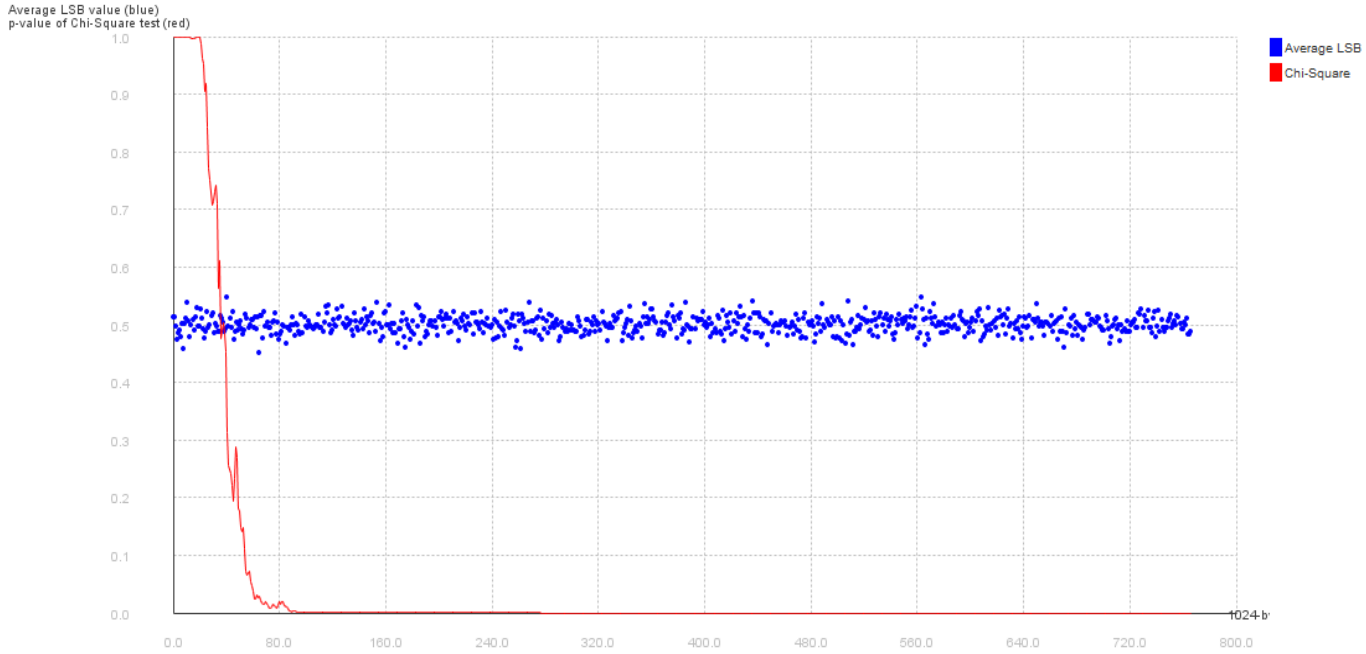

Figure 15: Chi-square attack from bottom to top on baboon stego image

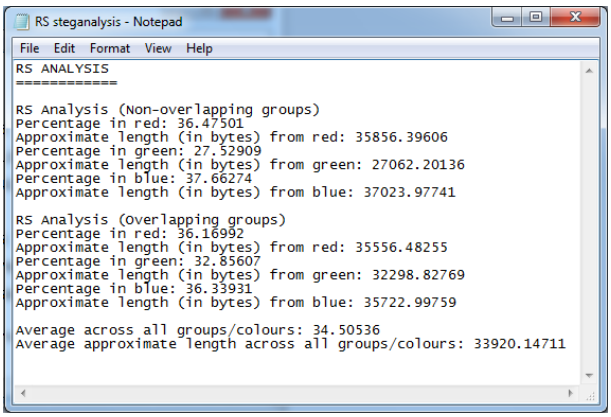

Figure 16: RS analysis on baboon stego image

- *Undetectability*: From the experimental results that have been carried out on all cover images, the PSNR values are greater than 70 db, while MSE values are very close to zero. Therefore, the undetectability of our steganographic method is achieved.
- *Robustness*: As proved in Sections 6.1, 6.2 and 6.3, the proposed steganographic method resists various kinds of sophisticated attacks.
- *Indistinguishability*: As mentioned in the analysis of undetectability, our steganographic method provides a high quality (PSNR) and a very small error rate (MSE) for all cover images compared with original images. Therefore, it is hard to distinguish between covertext and stegotext.
- *Security*: Assume that there is an attacker suspected in the stego-cover S_{txt}, then s/he performed statistical tests and discovered there is a hidden text into stego-cover S_{txt}, s/he cannot retrieve the hidden text h_{txt} because is stegoed using shared secret key. Thus, only legal user can destego the hidden text h_{txt}.

The comparison of hiding capacity and the obtained PSNR against [18, 24] are given in Table 7. From the table, the average hiding capacity and obtained PSNR of our steganographic method are more better than [18, 24].

Table 7: Comparison of hiding capacity achieved and the obtained PSNR

Cover image	Method	Hiding capacity (bits)	PSNR (db)
Lena	[18]	1,166,296	42.26
	[24]	2,045,260	42.40
	Our Method	3,547,174	55.67
Baboon	[18]	1,159,328	38.44
	[24]	1,956,789	38.25
	Our Method	2,822,323	56.39
Peppers	[18]	1,167,960	42.28
	[24]	2,110,148	41.99
	Our Method	4,272,027	55.03
Jet	[18]	1,165,184	42.60
	[24]	2,056,879	42.24
	Our Method	2,336,136	45.86
Avg.	[18]	1,164,692	41
	[24]	2,042,269	41
	Our Method	3,244,415	53

7 Conclusion

Public-key steganography allows two parties that have no prior knowledge of each other to communicate covertly over public channel. In this paper, we construct efficient certificateless public key steganography based on Distributed Discrete Wavelet Transform (DDWT) and Singular Value Decomposition (SVD). The experimental results show that the proposed steganographic method resists various kinds of sophisticated attacks. Furthermore, our scheme satisfies all stegosystem security requirements. Meanwhile it improves computational costs and communication overheads.

References

[1] S. Ahadpour, M. Majidpour, and Y. Sadra, "Public key steganography using discrete cross-coupled chaotic maps," *arXiv preprint arXiv: 1211.0086*, 2012.

[2] L. von Ahn, N. J. Hopper, "Public-key steganography," in *Advances in Cryptology (EUROCRYPT'04)*, LNCS 3027, pp. 323–341, Springer, 2004.

[3] S. S. Al-Riyami, and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of the Cryptography (Asiacrypt'03)*, LNCS 2894, pp. 452–473, Springer-Verlag, 2003.

[4] R. J. Anderson and F. A.P. Petitcolas, "On the limits of steganography," *IEEE Journal of Selected Areas in Communications*, vol. 16, no. 4, pp. 474-481, May 1998.

[5] M. Backes and C. Cachin, "Public-key steganography with active attacks," in *Proceedings of the Second International Conference on Theory of Cryptography (TCC'05)*, pp. 210–226, 2005.

[6] J. Baek, R. Safavi-Naini, W. Susilo, "Certificateless public key encryption without pairing," *Information Security*, pp. 134–148, 2005.

[7] D. Boneh, M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[8] R. P. S. Chauhan, R. Dwivedi, S. Negi, "Comparative evaluation of DWT and DT-CWT for image fusion

and de-noising," *International Journal of Applied Information Systems*, vol. 4, no. 2, pp. 40–45, 2012.

[9] P. Guillon, T. Furon, P. Duhamel, "Applied public-key steganography," in *Proceedings of Electronic Imaging*, pp. 38–49, 2002.

[10] D. He, J. Chen, J. Hu , "A pairing-free certificateless authenticated key agreement protocol," *International Journal of Communication Systems*, vol. 25, no. 2, pp. 221–230, 2012.

[11] D. He, J. Chen, R. Zhang, "An efficient identity-based blind signature scheme without bilinear pairings," *Computers & Electrical Engineering*, vol. 37, no. 4, pp. 444–450, July 2011.

[12] N. J. Hopper, *Toward a Theory of Steganography*, Ph.D. Thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, 2004.

[13] S. Katzenbeisser, F. A. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, Inc., Norwood, MA, USA., 2000.

[14] T. V. Le, "Efficient provably secure public keysteganography," *IACR Cryptology ePrint Archive*, article 156, 2003.

[15] T. V. Le, K. Kurosawa, *Efficient Public Key Steganography Secure Against Adaptively Chosen Stegotext Attacks*, Technical Report, Florida State University, 2003.

[16] T. V. Le, K. Kurosawa, "Bandwidth optimal steganography secure against adaptive chosen stegotext attacks," in *8th International Workshop on Information Hiding (IH'06)*, LNCS 4437, pp. 297-313, Springer-Verlag, 2007.

[17] C. H. Lin, J. S. Jen, and L. C. Kuo, "Distributed discrete wavelet transformation for copyright protection," in *The 7th International Workshop on Image Analysis for Multimedia Interactive Services*, pp. 53–56, 2006.

[18] J. K. Mandal and D. Das, "Colour image steganography based on pixel value differencing in spatial domain," *International Journal of Information Sciences and Techniques*, vol. 2, no. 4, pp. 83–93, July 2012.

[19] T. Ruffing, J. Schneider and A. Kate, "Identity-based steganography and its applications to censorship resistance," *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pp. 1461–1464, 2013.

[20] S. A. Seyyedi, V. Sadau and N. Ivanov, "A secure steganography method based on integer lifting wavelet transform," *International Journal of Network Security*, vol. 18, no. 1, pp. 124–132, Jan. 2016.

[21] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology (Crypto'83)*, pp. 51-70, 1984.

[22] R. S. Stankovic, B. J. Falkowski, "The Haar wavelet transform: its status and achievements," *Computers & Electrical Engineering*, vol. 29, no. 1, pp. 25–44, 2003.

[23] V. Strumpen, H. Hoffmann, A. Agarwal, *A Stream Algorithm for the SVD*, Massachusetts Institute of Technology, Computer Science and Artificial Intelligence Laboratory, 2003.

[24] P. S. Vitthal , B. S. Rajkumar , P. R. Archana, "A novel security scheme for secret data using cryptography and steganography," *International Journal of Computer Network and Information Security*, vol. 2, pp. 36–42, 2012.

[25] A. Wahaballa, O. Wahballa, F. Li, M. Ramadan, Z. Qin, "Multiple layered securities using steganography and cryptography," *International Journal of Computers and Applications*, vol. 36, no. 3, 2014.

[26] S. Wang , Z. Cao, H. Bao, "Efficient certificateless authentication and key agreement (CL-AK) for grid computing," *International Journal of Network Security*, vol. 7, no. 3, pp. 342-347, Nov. 2008.

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 Post-doctoral 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.

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).