A Hybrid Technique based on RSA and Data Hiding for Securing Handwritten Signature

Yaser Maher Wazery[1], Shimaa Gamal Haridy[2], AbdElmegeid Amin Ali[3]
Faculty of Computers and Information, Minia University

***Abstract*—Data exchange has been significantly encouraged by the development of communication technology and the wide use of social media over the Internet. Therefore, it is important to hide the data transmitted, especially the data that requires a person's signature. Where the signature is an increasingly needed item that is used in our daily life to achieve some paper-based authentication in departments, the individual himself needs the signature. Cryptography and steganography are commonly considered to be the most important data hiding methodologies. Steganography is used to hide the secret message in the carrier media, such as text, audio, video, and image files, without the carrier media being distorted, and cryptography is used to conceal the purpose of the secret message. A hybrid data hiding (image steganography) and encryption technique is implemented in this research on the time domain. The secret handwritten signature image is first encrypted using the public key algorithm (RSA) in the proposed technique, then randomly inserted using Embedding data process to be concealed in one of the last three bits of that pixel(1^{st} Least Significant Bit, 2^{nd} LSB, and 3^{rd} LSB) based on mathematical randomized formula over all pixels of the carrier media (image). It is assumed that the process of randomization will increase the protection provided by the technique. The suggested technique is implemented on gray level cover images. As a consequence of the random scattering of bits and using encryption, it is noted that the proposed technique achieves enhanced data hiding results in terms of performance, protection, and imperceptibility properties and the histogram of the proposed technique is better and provides more protection and security than the ordinary sequential Least Significant Bit (LSB).**

Keywords*—*Image Steganography; LSB; Data Hiding; Security; Embedding data; Cryptography; RSA; Handwritten signature

I. Introduction

With the exponential growth of technology, digital communication and social media, data protection has become very critical. In data communication, security problems during transmission are required to dealt with it. The specifications of secure communications are therefore important. Reliable personal identification/authentication is important because of the increasing importance of security technologies. The need for safety and access restrictions is important to safeguard the data transmitted, especially data that requires person's signature. Where the signature is an increasingly needed item used in our daily life to achieve some paper based authentication in departments. So in order to protect information over communication networks, there are two common types of techniques: cryptography and hiding information [1], which typically complement each other. The term hiding can either make the information undetectable (as in watermarking) or keep the information hidden (as in steganography). On the other hand, cryptography [2] is a method used to maintain the confidentiality of the content of the message. For the purpose of encrypting and decrypting sensitive data, several different approaches have been suggested and implemented.

- **Cryptography has two classification types:**
  - Classical cryptography: In this category the letters of the original message are encoded using either substitution techniques (each letter is replaced with another letter depending on key) or transposition techniques (reorder the letters of the original message to obtain the cipher text).
  - Modern cryptography: There are two types of algorithms in this category, (symmetric and asymmetric encryption).

Symmetric Encryption: The sender and the receiver must have the key to encrypt or decrypt message respectively. The symmetric encryption [3] has one key in the two sides for the message, so the sender conceals the message using a shared key with the receiver and the receiver decrypt the message using the same shared key.

Asymmetric Encryption (Public Key Cryptography): This approach has two different keys (private and public) used for the message encryption and decryption. Anyone can know the public key, and it can be used to encrypt messages and check signatures. Although the receiver is only aware of the private key, it is used to decrypt messages and sign signatures [4], as seen in figure 1.

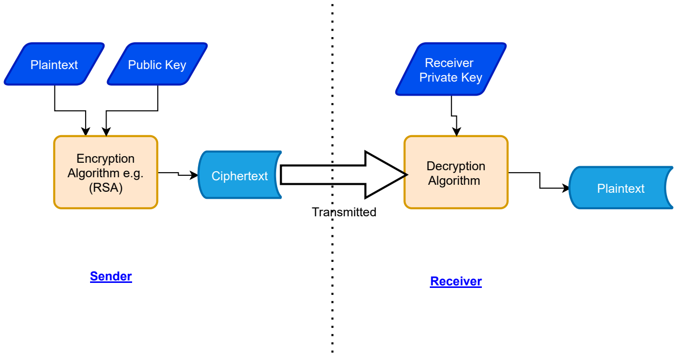


Fig. 1. Public Key Cryptosystem.

The use of public key cryptosystem like RSA provides the following advantages:

- The encryption key is public and distinct from the decryption key in a public-key cryptosystem, which is kept secret (private) but both are mathematically related.

- An RSA user generates and publishes, along with a supplementary value, a public key based on two large prime numbers. The prime numbers are secretly stored.
- Via the public key, messages can be encrypted by anyone, but can only be decoded by someone who knows prime numbers and private key.
- RSA's protection relies on the practical complexity of factoring two large prime numbers (factoring problem) into the product and modular arithmetic.

Steganography uses a carrier medium such as text, video, image, and audio file to cover the hidden data, according to figure 2. It is must for steganography to have some message to be embedded [5] and a cover medium in which the embedded message is hidden.

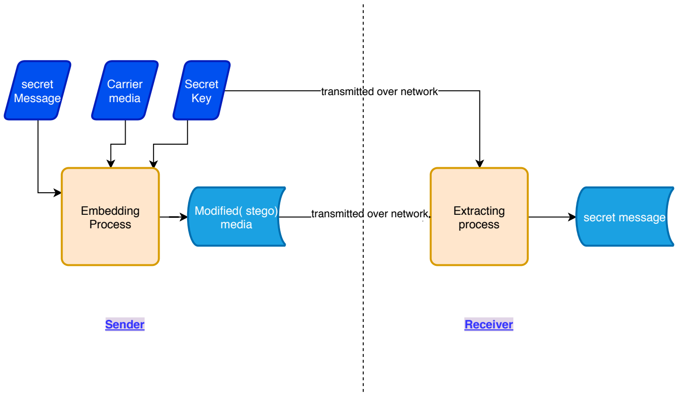


Fig. 2. Steganography Model.

The system of steganography should satisfy imperceptibility, high capacity and security[6], the key factors that influence steganography and its usefulness are these three aims. The accuracy of the image is also a significant objective for steganography. Two widely recognized methods are available to measure image quality: the Peak Signal-to-Noise Ratio (PSNR) and the Mean Squared Error (MSE) indicators. In such a case, PSNR is generally used to precisely detect the degree of corruption in the changed images compared to the carrier media. Whereas MSE is the solution to explain the distinction between two distinct images. Equations 1 and 2 [7] define MSE and PSNR.

$$MSE = \left(\frac{1}{S}\right)\sum_{i=1}^{S}(Z_i - Z'_i)^2 \quad (1)$$

$$PSNR = 10\ \log_{10}\frac{I^2}{MSE} \quad (2)$$

Where $Z_i$is the index of the i^{th} cell pixel in the carrier image, Z'_i is the index of the i^{th} cell pixel in the modified image, where the parameters S is meant to be the size of the both images and I is the upper bound of the pixel value, for gray level images (8-bits per pixel), I = 255.

The protection obtained by steganography to mask sensitive data inside a cover media depends on the presumption that no one may assume any secret data is available. However, if someone discovers a difference in the cover media [8], it is possible to discover sensitive data. Therefore, before concealing it in the cover media, it is preferred to use another approach such as cryptography to encrypt the sensitive data, this would ensure that even though the embedded data is found [9], no one will know its meaning. Therefore, we should take advantage of hybridization the two strategies for better protection. In general, steganography is the science of hiding information through a certain process in another type of cover media, i.e. text, video, audio and image[2]. While cryptography is the technique that use mathematics to convert intelligible data into unintelligible form to keep messages safe. The main description of steganography process is shown in figure 1. This study focuses on Cryptography and Steganography based on images where the embedding is done with the encrypted key concealed in the Object cover after encrypting the message. As the other layer of this encryption scheme, cryptography primarily encrypts the hidden plain text / image, converting it to cipher text/ image.

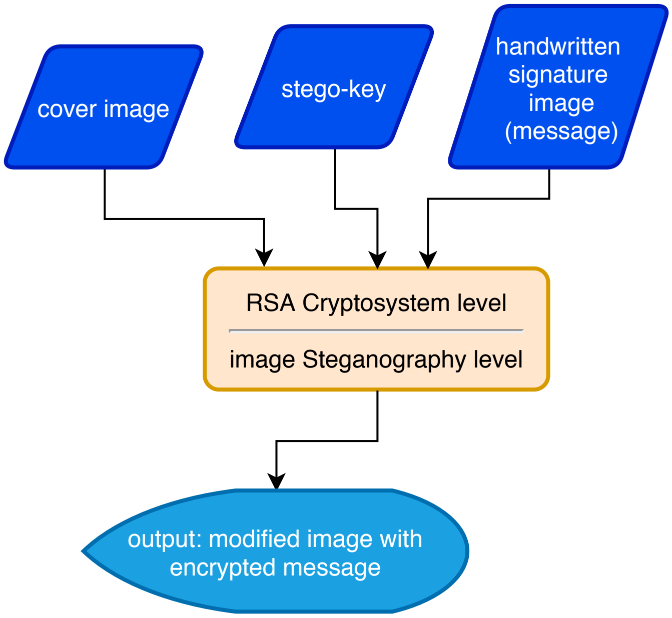

cover image
stego-key
handwritten signature image (message)
RSA Cryptosystem level
image Steganography level
output: modified image with encrypted message

Fig. 3. Proposed Model.

This study introduces a 2-level protection framework for crypto-stego using steganography of the image base as a dependent level and cryptography of RSA as an independent assurance level. The sensitive data passes through the crypto level in the proposed security strategy, followed by the steganography level, which results in the output file as Stegoimage. The main description of the process using these two level techniques is shown in Figure 3. In this paper a security technique based on steganography and public key (RSA) encryption as two levels is proposed. The cover media is a gray level image. The cover image is hiding the secret ciphered message (handwritten signature) by RSA using a modified scattered Least Significant Bit (LSB). The most common types of images used in our daily life situations for handling paper based work is gray level imaging after scanning because it is cheaper and available in most of places.

II. Literature Work / Review

In [10], by using scattered LSB, the authors implemented a technique that hides a fingerprint image as (message) in a face image as (covered image). They first use a password to encrypt the fingerprint image bits, then embed those bits using LSB but not linearly, rather a pseudo random number generator (PRNG)[11] that depends on the password is used to pick the position of the pixel in which the bit would be inserted. By using this structure, without knowing the password, it is not possible for anyone to try reading the secret data to get the hidden version (not even the encrypted version). The observations of this proposed technique explained that scattered LSB introduces a large value of PSNR comparing to sequential LSB, which means image quality of scattered LSB is higher than of the values obtained by sequential LSB.

In [7], they presented a method that arbitrarily (depending on the mathematical equation) embeds the character of the secret message into the carrier media in just three pixels. A colored picture reflecting three levels (Red, Green , and Blue) is the carrier media. During the first iteration, only two tiers (Green and Blue) are used in the embedding operation. In the second iteration, only the blue tier should be included. Two more stages (Green and Blue) and one stage (blue tier) are used in the following iterations and so on. The use of this approach leads to protection improvements and better performance for PSNR values. The secret information embedding is performed randomly. The pixel position decision is made by means of a PRNG [12] rather than ordinary linear matter. The message bits must be hidden in a shape of (3-2-3) during the insertion process. Where the first 3-bit of the original message is entered at the first random position of the pixel ((2-bit of the blue level at (7^{th} bit) and bit at (8^{th} bit)), (and the third bit of the 3-bit of the green level is inserted at the 8th position of the message). Then, in the place of the second random pixel (7^{th} bit) and (8^{th} bit) of the Blue level, the successor 2-bits obtained from the original message (4^{th} and 5^{th} bits) are entered. After that, in the third random pixel location ((2-bits in the blue level at (7^{th} bit) and (8^{th} bit)), (1-bit at (8^{th} bit) of the green level), and so on, the final 3-bits obtained from the original message (6^{th}, 7^{th} and 8^{th} bits) should be added. The outcomes of the proposed method explains that it incorporates greater PSNR value and greater ability for embedding than sequential LSB.

A hybrid data hiding (HDH) technique applied to the medical imaging field was suggested by the authors in [13]. HDH combines Hamming (3, 2) + 1 and original LSB techniques with the Optimal Pixel Adjustment Process (OPAP) system used to encode patients' secret information. HDH strengthens the process of 'Hamming + 1'. Moreover, the output and the capability of changing The photos have been enhanced. Comparing to other similar techniques, the results of the implemented approach showed an enhancement in the hiding ability carried out by this technique. In addition, the accuracy of the updated images remained greater than 50 dB in the medical sector for the proposed scheme images.

In [14], the authors suggested new and creative audio steganography for the purpose of popularizing the use and products of IoT services. The proposed solution provides a more stable IoT climate. This study focuses on audio steganography, concentrating on the hidden message followed by the adoption in the originally provided audio stream of the optimized audio embedding technique (OAET) for shuffling bit embedding replacement. for concealing the hidden message, a random bit selection is applied by the technique used in[14] to conceal the necessary data in the farthest part of the audio stream. Their suggested technique showed improvements in the robustness of the inserted audio stream, and the outcomes showed a decrease in the distortion impact. The process uses WAV as the default format for the original stream of audio. The results of this paper also showed that the quality of the audio file is better than the standard LSB after implementing the proposed technique, and provides high-level protection.

In [15], the authors suggested an improved method to protect confidential personal computer text data that benefits from the combination of(cryptography and steganography). The protection of the system is provided by the inclusion of RSA cryptography followed by video based steganography as two sequential layers to ensure the best possible safety. The implementation of the framework starts with the user entering a secret confidential text data message and a secret key for the cryptography level The software transforms each character of the confidential secret text within this level method into an array of binary to be encrypted using RSA. The second level, i.e. the steganography level, also demands the cover media for an RGB video frame, so that its pixels are also transformed into binary form. There are 3 channels of any pixel in the RGB video frame (red , green and blue) displaying a byte of each. The authors used 3 bits of hidden data to be embedded in each pixel using the least significant bits (LSB) of video-based steganography in their paper. In order to explore the relationship between protection, capability and data dependence, the study modeled the system and implemented it for testing. The experiments involved testing of data protection in 15 different video sizes that yielded interesting results in comparison with the existing method in [16]. this study reinforced capability vs. security, as an inevitable trade off was implemented. The tests included all possibilities for using number of bits to be concealed in one pixel (1-LSB, 2-LSB, and 3-LSB) security acceptance methods describing their impact on the cover video. The major result proved applicable to the implementation of the 3-LSB approach to provide acceptable protection with realistic capacity preferred between 1-LSB and 2-LSB methods.

In [17], the authors suggested a hybrid technique to secure the secret data that use the behaviors of steganography (LSB, raster scan technique) and cryptography (symmetric key). Using a symmetric key cryptography technique, which is content-based and uses the block cypher principles, the secret text will first be encrypted, but the size of the block in this technique is not determined, depending on the length of the term (word). Secondly, the embedding process for ciphered data in RGB carrier image at the 3 planes R, G and B is occurred as follows: Using modified LSB replacement by XORing hidden data bits with cover pixel bits, 2 bits will be embedded in 2 LSB red plane, then 2 bits will be inserted using raster scan technique in 2 LSB of green plane (hide from left to right in the first scan and right to left in the next scan and so on) by XORing hidden data bits with covering pixels, then using raster scanning technique (hide from top to bottom in the first scan and from bottom to top in the next scan and so on) 4 bits will be inserted in 4 LSB of blue plane by XORing hidden data bits with bits of cover pixels. This process is repeated until the entire text of the cipher is concealed in the carrier image. The statistical results provide that no observation difference between the cover image and the Stego image. In analysis method, MSE and PSNR parameters are calculated and correlated with the performance of current technique [18], and the results show that the proposed work has variability in the PSNR and the degree of protection is also very high.

In [19], the authors suggested a hybrid technique to secure the image and text using the combination of cryptography and steganography (RSA, LSB and DWT). In this research, a gray level image is taken as a carrier image, then the replacement of the LSB bits on the cover image is applied after choosing the cover image. Using the RSA encryption method, the secret data will be translated into cipher text behind the encrypted image, the encrypted text is concealed. So The original message is protected by two layers of security. Firstly, the secret message itself is encrypted, and then the cover image is encrypted as well. It's then inserted in the original image. The LSB extraction method is used in the decoding process to get the message bits. The bits are then removed from the location in the same order as they were embedded, when the position of the bits has been defined. Extract encrypted images from the DWT cover image and decrypt text with the private key of the recipient using the RSA technique. The results show that MSE of images used is less by comparing the MSE values of all images, and PSNR of images is higher than the present technique [17] in the proposed technique. The result of images derived from entropy indicates that the entropy of the modified image is relatively higher than the cover image. This is due to the inclusion of more secret details to the cover image.

In [20], the authors suggested a scheme to produce a reliable and stable message transfer technique such that private and confidential information can be transmitted over the network in a secure manner. The proposed method is applicable to gray scale images. The pixels' 7^{Th} bit is subjected to a mathematical function. The 7^{Th} bits of the selected pixel and the pixel $+1$ value are obtained, and 2 bits of the message can be extracted from each pixel using a combination of these two values. 00, 01, 10, and 11 are the four possible variations. This approach has many benefits, including two bits of message are stored in each pixel and the technique's independence from the 8^{Th} digit. When inserting the data into the image file, the pixel value will shift by a maximum of $+2$ and -2. The results when compared to other approaches, show a high PSNR and a low MSE.

III. The Proposed Technique

The proposed technique for securing and hiding the handwritten signature image is illustrated and clarified in this section.

The proposed scheme's goal is to create a safe and robust message transfer technique such that private and sensitive information (handwritten signature) can be transmitted over the network in a secure manner without being vulnerable to unintended recipients and attacks. The proposed method is applicable to gray scale images. We introduced a multilevel security paradigm first by securing through RSA then providing a sophisticated embedding by applying a randomized positioning for choosing cover media bit's position and value. The proposed technique can be described as two stages; the first one is encrypting the handwritten then embedding / inserting and the second is extraction and restoring the handwritten signature image. This technique aids in overcoming steganography's weaknesses in traditional LSB to a greater degree. Embedding Algorithm & Extraction Algorithm are shown in figures 4, 5 respectively.

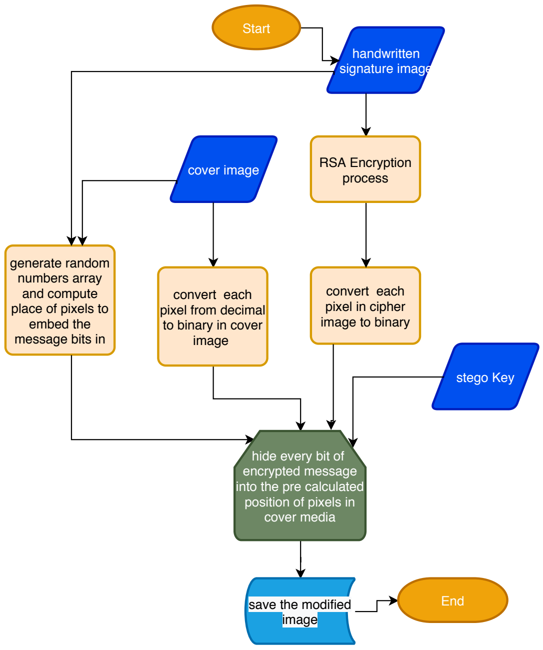

Start
handwritten signature image
cover image
RSA Encryption process
generate random numbers array and compute place of pixels to embed the message bits in
convert each pixel from decimal to binary in cover image
convert each pixel in cipher image to binary
stego Key
hide every bit of encrypted message into the pre calculated position of pixels in cover media
save the modified image
End

Fig. 4. Encryption and Embedding the Handwritten Signature Image Process.

A. Encrypting and Embedding Stage

The first algorithm will be used to conceal the secret handwritten signature as image randomly (depending on a mathematical equation) in the (1^{st} LSB, 2^{nd} LSB and 3^{rd} LSB) over the carrier media which is a gray level image after encrypting using RSA encryption Algorithm. The inputs of the insertion algorithm are the handwritten signature's image and the carrier media; the first technique is divided into two parts (Encryption using RSA and embedding using modified LSB):

1) RSA Encryption: The RSA algorithm is a method of public key encryption and is known as the most secure form of encryption. It was invented in 1978 by Rivest, Shamir and Adleman, the RSA algorithm has the name of them. The steps of encrypting the handwritten signature image are shown in figure 6 and the algorithm is shown in (algo: 1).

Algorithm 1: RSA Encryption

```
Input: Handwritten signature image;
Output: Ciphered signature array;
First, the two key pairs (public and private) are generated by:
Selecting two different prime numbers ($aandb$).
Calculate the product for public and private keys ($n$) by the equation [21]:
    $n = a * b$    (3)
Calculate the totient ($\phi(n)$) [21]:
    $\phi(n) = (a - 1) * (b - 1)$    (4)
Select an integer value $e$ for public Key, such that
$1 < e < \phi(n)$ and ( $e$ , is relatively prime to $\phi(n)$) if they share no common factors other than 1; $gcd(e, \phi(n)) = 1$.
Calculate the private key d to fulfill the congruence relation $e.d \equiv 1 (\mod \phi(n))$.
The modulus n and the encryption exponent e generate the public key.
$a, b$ and the private exponent $d$ generate the private key which must be kept secret.
The handwritten signature image is converted to one dimension array of decimal numbers.
then is encrypted using RSA public key by RSA encryption equation [21]:
for $i = 1 \leq message_{L}ength$ do
    $C_{handwritten}(i) = (M_{handwritten}(i))^{e} \mod n;$    (5)
end for
where $C_{handwritten}$ is the handwritten signature after applying RSA encryption and $M_{handwritten}$ is the main handwritten signature.
return ciphered handwritten array;
```

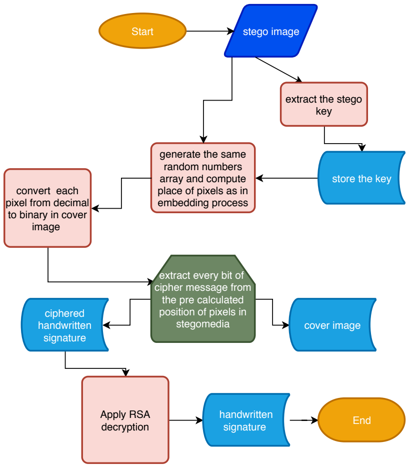

Start
stego image
extract the stego key
store the key
generate the same random numbers array and compute place of pixels as in embedding process
convert each pixel from decimal to binary in cover image
extract every bit of cipher message from the pre calculated position of pixels in stegomedia
ciphered handwritten signature
cover image
Apply RSA decryption
handwritten signature
End

Fig. 5. Extraction and Decryption the Handwritten Image Process.

2) Embedding using Modified LSB: After making RSA encryption the cipher handwritten signature are entered to the embedding algorithm with the 16-bit carrier cover image and a secret key, the algorithm is stepped in (algo: 2) .

Algorithm 2: Embedding using Proposed LSB

```
Input: Ciphered handwritten image, Cover image, Stego-key;
Output: Stego image;
Each pixel of ciphered handwritten signature's is converted from decimal to binary of 16-bit length generating $binary_{I}mage$.
Compute place of pixels $n_{B}locks$ to embed the message bits in (this random array is generated as the same in the destination side).
    $n_{B}locks = \frac{image_{L}ength}{s_{l}ength}$    (6)
Where $image_{l}ength$ is the size of cover image and $s_{L}ength$ is the size of handwritten image.
Generate and calculate the random array $R$ that ranges from $6to8$ the last three bits of LSB
    $R = \sum_{i=1}^{s_{L}ength} rand(6 : 8)$    (7)
The same R are generated at the extracting algorithm by using this matlab function: $rng(seed, generator)$ where $rng$ is a Control function that handles random number generation, Seed is the parameter used to seed the random number generator using a non-negative integer value, and a generator additionally specify the type of the random number generator.
Then the pixels of carrier media is transformed to its ASCII binary.
Calculate $N$ the length of the ciphered signature.
Convert the cover image matrix to column.
Initialize $k = 1$, $t = 1$;
for $i \leq image_{L}ength$ do
  if $k \leq N$ then
    Every bit of the handwritten signature's image is hidden after a calculated number of pixels' blocks from equation 6 at the last three bits LSB in the pixel of cover image randomly based on the equation 7.
    $Stego_{I}mage =$
    $LSB(R(t), cover_{I}mage(i), binary_{I}mage(k))$;
    Increment $k = k + 1$;
    Increment $t = t + 1$;
  end if
  Increment $i = i + n_{B}locks$;
end for
convert the column $Stego_{I}mage$ to matrix;
After hiding the signature, a secret key is hided into the modified image $Stego_{I}mage$ that is known for both sender and receiver to be able to extract the handwritten signature image after receiving.
write the new image($Stego_{I}mage$)
```

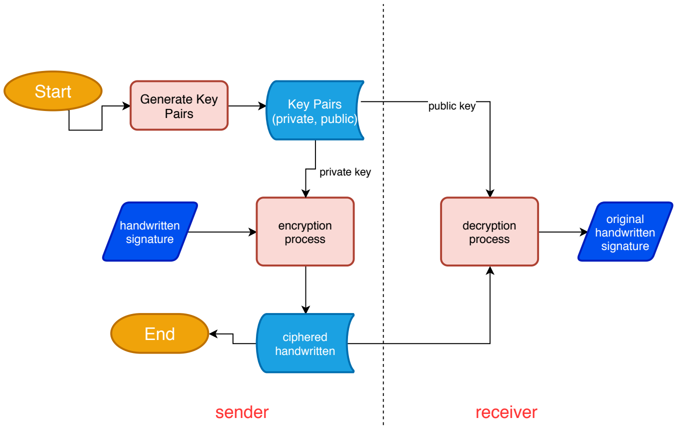


Fig. 6. RSA Model.

B. Extracting and Decrypting Stage

The second algorithm will be used to extract the ciphered secret handwritten signature form a stego-image using the same random numbers those are generated in the embedding process (depending on a mathematical equation) over the modified gray level image and then decrypting it using RSA decryption Algorithm. The second stage is divided into two parts (extracting using modified LSB and decrypting using RSA which are shown in algo: 3 and algo: 4):The inputs to the extraction algorithm are (the $stegokey$ and the $Stego-image$) for extraction and (private key of RSA (d, n)) for decryption.

1) Algorithm of Extraction part:

2) Algorithm of Decryption part:

IV. Experimental Results

The use of RSA cryptosystem in the proposed technique is according to:

- A key exchange is not necessary in asymmetric RSA and this improves the security of the algorithm.
- For the cryptographic process, RSA uses factorization that significantly decreases the algorithm's speed.
- Much faster than RSA are symmetric algorithms but a protected encryption scheme (Cryptosystem as RSA) is needed to protect against brute force attacks and differential plaintext-cyphertext attacks. The handwritten signature is important to be secret during transmission so the RSA is used.

The covered images used are 8-bit gray scale images. The handwritten signature images to be encrypted and hidden are taken from a data-set in[1] kaggle website[22]. The cover image contains information about the hidden file, such as hidden file size. While developing the technique the concern was about four different sizes of cover images (papers of size A4, A3, A5) and a template cover images are used such as (Lena, Pepper and Pears) of size 512*512, and fixed size for handwritten signature image (40*80) are used of type uint16 to achieve more security after using RSA for bigger values. After

Algorithm 3: The Extraction algorithm

```
Input: $Stego-image$ and $Stego-key$;
Output: ciphered handwritten image as column;
exclude the message size from the $Stego-image$
depending on $Stego-key$.
convert the image to one array (column).
generate same random array to retrieve the bits and pixels
places of the embedding message ($1^{st}$, $2^{nd}$ or $3^{rd}$ LSB) to
calculate $RG$ (Random array of bits (6:8) from
equation (7)) and $no_Blocks$ (no. of blocks representing the
location of pixels that the message was embedded in, from
equation (6)) .
$k = 1$, $t = 1$;
for $i \leq imageLength$ do
   if $k(ismessageindex) \leq message_Length$ then
      $Stego_PixelBits$ = convert $stegoImage$ from decimal
      to binary of 8 bit length;
      $secret_Bits(k) = Stego_PixelBits(RG(t1))$
      increment $k = k + 1$;
      increment $t = t + 1$;
   end if
   increment $i = i + no_Blocks$;
end for
combine each 16 bit and add it in one pixel in
$secret_Image$ array.
define $tt = 1$;
define $index = 1$;
for $i = 1 \leq message_Length$ do
   for $j = 1 \leq 16$ do
      $Secret_Image(index) += secret_Bits(i)$;
      $j = j + 1$;
   end for
   $index = index + 1$;
   increment $i = i + 16$;
end for
convert the secret image array $Secret_Image$ from binary
to decimal.
```

Algorithm 4: RSA decryption

```
Input: Ciphered handwritten image array;
Output: Original handwritten image;
Then applying the RSA decryption using the private key
$(d, n)$.
for $i = 1 \leq messagelength$ do
   Calculate message by the equation of decrypting RSA
   [21]:
        $$M_{handwritten} = C^{d}_{handwritten} \mod n \qquad (8)$$
   $Calculatemessage(i) =$
   $power(cipheredSecret_Image, d)modn$;
end for
Convert the column array (message) to image (the original
handwritten signature image).
```

[1] https://www.kaggle.com/divyanshrai/handwritten-signatures

encrypting the handwritten signature using RSA, its bits does not use sequential LSB but it is distributed randomly according to the use of a PRNG that depends on the carrier media size and the handwritten signature image size. This PRNG determine two things: the placements of pixels in covered image to insert the handwritten image's bits and the bit number in that pixel to do scattered LSB.

A. PSNR value:

PSNR is defined as the ratio between the desired signal power and the noise signal power (signal that corrupts the main signal). A higher PSNR value shows that the image has better quality. PSNR value of the proposed technique was calculated for original and modified images and results are clarified in table I. While experimenting the proposed algorithm it was vital to compare its results to the ordinary LSB(1^{st} LSB) and the technique in [17]. The proposed technique is dealing with gray cover image which has less pixels than a color cover to embed the secret data, also it is dealing with last three bits of pixel (1^{st},2^{nd} and 3^{rd} LSB) randomly which has better security than sequential LSB (1^{st} LSB) so in the case of discovering the hiding message, the extraction of the proposed technique will be hard than using 1^{st} LSB and if it is extracted the message is encrypted using RSA. The MSE and PSNR value of the technique [17] was provided in comparison to the proposed and the 1^{st}LSB in tables II and III respectively. It is normal that PSNR of 1^{st} LSB has more value than any technique applied on other bit of LSB, also the PSNR of same embedding capacity that is applying on cover image is higher than embedding the same capacity on gray image, but the proposed technique is more concerned with the security of the handwritten signature. The results of the proposed technique is scaled using the same ratio of capacity to cover size in technique [17] to compare its results, since the authors of this technique used a colored cover image 3 levels (R,G,B) of size (512*512) and the proposed technique uses only one level (gray level) of size (512*512). Moreover, a proposed technique applied the l^{st} LSB on gray cover image to compare its results with technique [17], as this technique apply sequential LSB.

TABLE I. PSNR and MSE of the Proposed Technique in Different sizes of Covered Image and same size of Handwritten Image

Cover image template size	Cover image size	Handwritten signature image size	PSNR	MSE
A4	3508*2480	40*80*16 bit depth	64.8506	0.0213
A3	4961*3508	40*80*16 bit depth	67.8931	0.0106
A5	2480*1748	40*80*16 bit depth	61.9136	0.0419

TABLE II. MSE of the Proposed at Different Images Dataset (Applying on Handwritten Image) with Gray Cover Image and Existing Algorithms (applying on text) with Colored Cover Image in [17] and a Proposed Method Applying 1^{st} LSB on Gray Cover Image

Cover Image	Cover Size	Capacity of message	Proposed MSE	MSE in [17]	proposed MSE of 1^{st} LSB
lena.jpg	512*512	2K	0.3395	0.0211	0.0327
pears.png	512*512	2K	0.3235	0.0214	0.0323
peppers.jpg	512*512	2K	0.2242	0.0212	0.0322

The results in these tables show that the PSNR values for the proposed LSB is high for embedding 2 K bytes in the gray cover image than using the technique in[17] that embeds capacity of 2000 bytes and embeds those bits in color covered image i.e (it embeds more than bits in one pixel unlike our proposed technique that embeds only one bit in the pixel, the PSNR values of that proposed LSB is high as Typical values for the PSNR and lossy media compression has normal value of 30 and 50 dB, where higher value is better [7] and the value of PSNR obtained by the proposed LSB also has the acceptable range. The main concern of this research is about security; the use of hybrid Cryptography RSA and proposed steganography LSB is more secure than using only steganography sequential LSB for using two parameters: randomizing in place of pixels for inserting the bit of handwritten signature and randomizing in selection of number of bit in that pixel to do bit scattering (not normal LSB, but random in range of last three bits).

TABLE III. PSNR of the Proposed Method at Different Images Dataset (Applying on Handwritten Image) with Gray Cover Image and Existing Algorithms [17](Applying on Text) with Colored Cover Image and a Proposed Method Applying 1^{st} LSB on Gray Cover Image

Cover Image	Cover Size	Capacity of message	Proposed PSNR	PSNR in [17]	proposed PSNR of 1^{st}LSB
lena.jpg	512*512	2K	52.82	64.89	62.98
pears.png	512*512	2K	53.03	64.83	63.03
peppers.jpg	512*512	2K	54.62	64.88	63.05

B. Entropy:

A further parameter is also used to evaluate the cover image and stego image in table IV, i.e. Entropy (Average content for information). It tests the proportions of the picture's data. It is commonly calculated as bits in units.

$$Ent(p) = \sum_{i=0}^{T} Pro(i) \log Pro(i) \tag{9}$$

where $pro(i)$ is the function of a given image's probability density at intensity level l, and T is the total number of grey levels in the image. An picture with a high value of entropy is known as having better quality and high information. The entropy's values shown in table IV provide that the proposed technique stores more information at the cover images than the existing technique, as our model deals with a handwritten image as a secret data of large capacity due to using the RSA encryption before embedding it rather than using text of small capacity in [19].

TABLE IV. Entropy's of Cover Image and Modified (stego) Image

image of size (512*512)	Cover image's Entropy	modified image's Entropy	Cover image's Entropy in [19]	modified image's Entropy in [19]
lena.jpg	7.4482	7.4503	7.4469	7.4470
pears.png	7.2591	7.2600	7.2587	7.2588
peppers.jpg	7.5903	7.5918	7.5818	7.5819

TABLE V. PSNR OF PROPOSED METHOD AND OTHER TECHNIQUES BY HIDING $8KB$ OF DATA IN IMAGES OF $(256*256)$.

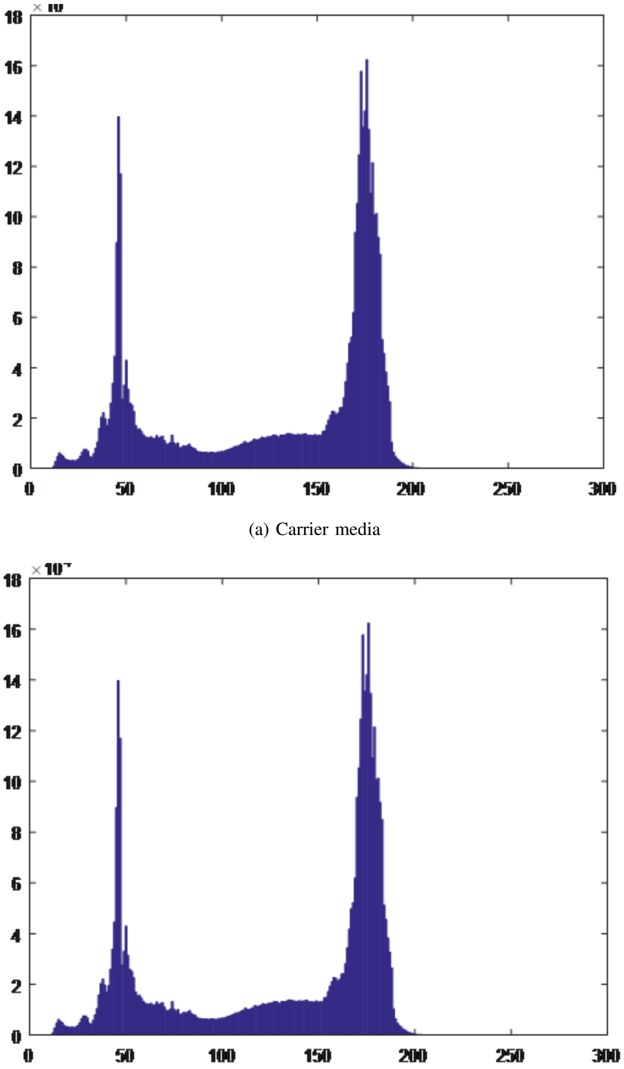
Image name	Classic LSB method in [23]	Method in [20]	Proposed Method
Lena	42.51	49.37	45.22
Baboon	54.73	49.38	45.65
Pears	43.24	49.41	45.34

C. Comparison between Proposed method and other techniques

The value of PSNR for the proposed method is compared to that of various methods, with the results shown in Table V. The 8 KB message data(ciphered handwritten image in proposed method) is converted to binary and applied to standard images with a resolution of 256*256. Table V displays the effects of various techniques' PSNR values when applied to different images; the PSNR values for the other technique are taken from [23] and[20]. The LSB approach is simple to deconstruct. The method in [20] provides more capacity, but the proposed method is concerned with security more than capacity.The proposed method provides more security due to applying cryptography and hiding data in one of the last three bit randomly and not sequential.

D. Histogram analysis:

The image histogram is computed for the carrier media and the modified image and clarified in figures 7a, 7b, 8a, 8b and 9a, 9b. Where in figure 7a a carrier media is used having A5 paper size and it clarifies the histogram of carrier media at the left and the histogram of the modified image in figure 7b after applying the proposed technique of embedding at the right, in figure 8a a Pepper cover image of size 512*512 is used it shows histogram of covered image at the left and the histogram of the modified image in figure 8b after applying the proposed technique of embedding at the right and in figure 9a an Lena cover image of size 512*512 is used and it shows histogram of covered image at the left and the histogram of the modified image in figure 9b after applying the proposed technique of embedding at the right. The histograms of both the images (covered and stego) are quite similar where the histogram of proposed technique has no difference from the carrier media rather than the sequential LSB which there exist some difference between the carrier image and the modified image of that technique. Hence the proposed technique is found to be outperforming in comparison to existing techniques.



(a) Carrier media

(b) Modified-Image

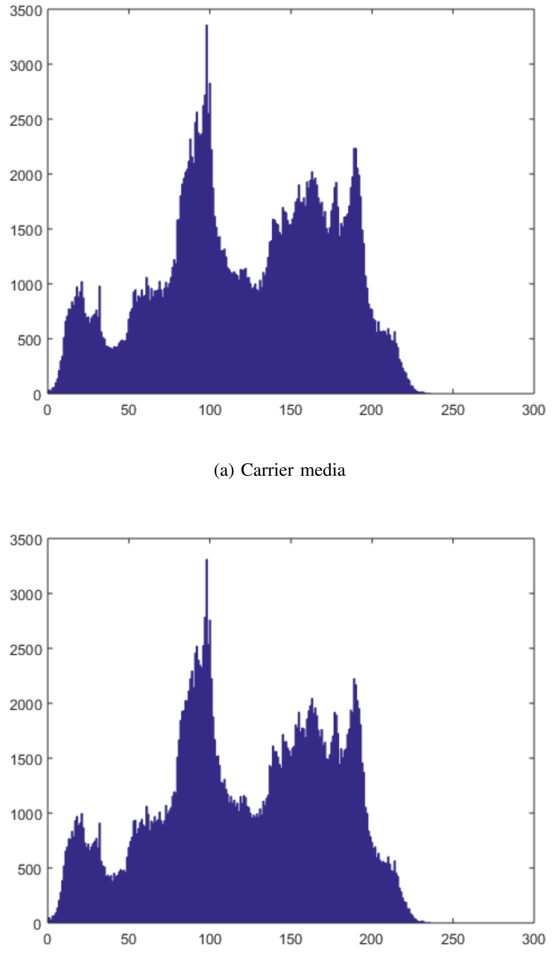
Fig. 7. Histogram Proposed Technique of LSB Embedding with Size A5.

V. CONCLUSION

Signature is an important matter that is used in our daily life to accomplish any authentication for papers in work environment needing the signature of the person himself. There are many techniques for securing the data such as cryptography and steganography (like spatial domain, Transform domain). Cryptosystem and spatial domain is the area of interest in this research. The usage of the public key cryptosystem like (RSA) in hybridization with steganography provides more enhanced paradigm for securing the process of hiding human handwritten signature. In this research, we proposed such a paradigm that uses RSA in conjunction with scattering LSB based on precalculated random mathematical equation. The main concern of the proposed technique is about securing handwritten signature based on cryptosystem (RSA) and steganography, using modified LSB (scattered LSB in choosing pixel place and randomly choosing bit number to do LSB), rather than using sequential LSB. In contrast to the LSB method, our method does not consider its dependence on the 8th bit. One of the most important requirements of steganography is to embed the hidden message inside the carrier image without altering it significantly. Our method also meets this criterion to a higher degree. The experimental results show enhancement of PSNR value and histogram, the overall security of the scattered distribution provides an advanced security scheme comparing to the fixed allocation LSB.

REFERENCES

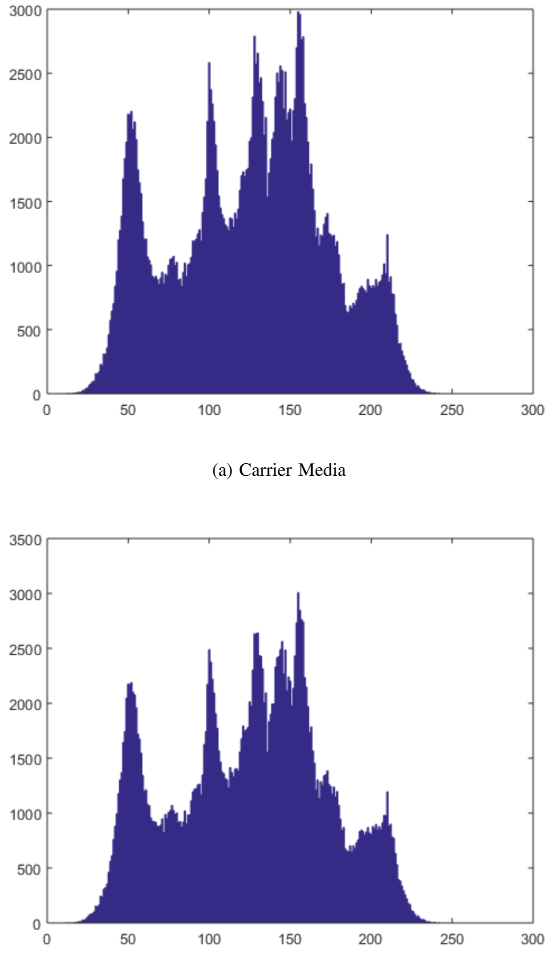
[1] D. P. M. Vijay Kumar Sharma, Dr. Devesh Kr Srivastava, "A study of steganography based data hiding techniques," *International Journal of*



(a) Carrier media

(b) Modified-Image

Fig. 8. Histogram Proposed Technique of LSB Embedding with Pepper Cover Image of Size 512*512



(a) Carrier Media

(b) Modified-Image

Fig. 9. Histogram - Proposed Technique of LSB Embedding with Lena Cover Image of Size 512*512.

Emerging Research in Management and Technology, 2017.

[2] N. B. Dipti Kapoor Sarmah, "Proposed system for data hiding using cryptography and steganography," *International Journal of Computer Applications*, 2010.

[3] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, "A survey on the cryptographic encryption algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 11, pp. 333–344, 2017.

[4] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of steganography and cryptography: A short survey," in *IOP conference series: materials science and engineering*, vol. 518, no. 5. IOP Publishing, 2019, p. 052003.

[5] S. M. H. Mohammad Ajman Hossain, "Steganography techniques: A review paper," *International Journal of Contemporary Computer Research (IJCCR)*, 2017.

[6] G. K. Rashmeet Kaur Chawla, "Comparative study on different steganographic techniques," *International Journal of Scientific Research and Management (IJSRM)*, 2015.

[7] F. A. O. Marwa M. Emam, Abdelmgeid A. Aly, "An improved image steganography method based on lsb technique with random pixel selection," *International Journal of Advanced Computer Science and Applications (IJACSA)*, 2016.

[8] F. A. O. Marwa E. Saleh, Abdelmgeid A. Aly, "Data security using cryptography and steganography techniques," *International Journal of Advanced Computer Science and Applications (IJACSA)*, 2016.

[9] T. S. S. S. Manisha, "A two-level secure data hiding algorithm for video steganography," *Multidimensional Systems and Signal Processing*, 2019.

[10] I. S.Brindha, "Hiding fingerprint in face using scattered lsb embedding steganographic technique for smart card based authentication system," *International Journal of ComputerApplications*, 2011.

[11] A. K. G. Unik Lokhande, "Steganography using cryptography and pseudo random numbers," *International Journal of Computer Applications*, 2014.

[12] K. H. Shamim Ahmed Laskar, "Steganography based on random pixel selection for efficient data hiding," *International Journal Of Computer Engineering and Technology (IJCET)*, 2013.

[13] C. Kim, D. Shin, B.-G. Kim, and C.-N. Yang, "Secure medical images based on data hiding using a hybrid scheme with the hamming code, lsb, and opap," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 115–126, 2018.

[14] J. E. Anguraj S, Shantharajah S P, "A steganographic method based on optimizedaudio embedding technique for secure datacommunication in the internet of things," *Computational Intelligence*, 2019.

[15] E. A. K. Nouf A. Al-Juaid, Adnan A. Gutub, "Enhancing pc data security via combining rsa cryptography and video based steganography," *JOURNAL OF INFORMATION SECURITY AND CYBERCRIMES*

RESEARCH (JISCR), 2018.

[16] N. A. Al-Otaibi and A. A. Gutub, “2-leyer security system for hiding sensitive text data on personal computers,” *Lecture Notes on Information Theory*, vol. 2, no. 2, pp. 151–157, 2014.

[17] S. Chauhan, J. Kumar, A. Doegar *et al.*, “Multiple layer text security using variable block size cryptography and image steganography,” in *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*. IEEE, 2017.

[18] A. Singh and H. Singh, “An improved lsb based image steganography technique for rgb images,” in *2015 IEEE International Conference on electrical, computer and communication technologies (ICECCT)*. IEEE, 2015, pp. 1–4.

[19] S. Bhargava and M. Mukhija, “Hide image and text using lsb, dwt and rsa based on image steganography.” *ICTACT Journal on Image & Video Processing*, vol. 9, no. 3, 2019.

[20] K. Joshi, S. Gill, and R. Yadav, “A new method of image steganography using 7th bit of a pixel as indicator by introducing the successive temporary pixel in the gray scale image,” *Journal of Computer Networks and Communications*, vol. 2018, 2018.

[21] W. Stallings, *Cryptography and network security, 4/E*. Pearson Education India, 2006.

[22] I. Vellore Institute of Technology University, “Handwritten signature dataset,” 2018, accessed Feb 2019. [Online]. Available: https://www.kaggle.com/divyanshrai/handwritten-signatures

[23] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, “A novel magic lsb substitution method (m-lsb-sm) using multi-level encryption and achromatic component of an image,” *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14 867–14 893, 2016.