Wavelet Based Pseudo Quantum Steganography within Pseudo Color Barcode

HIEU Q. NGUYEN, XIAODI WANG
Department of Mathematics
Western Connecticut State University
181 White Street, Danbury, CT, 06810
UNITED STATES OF AMERICA
nguyen084@connect.wcsu.edu xiaodiwang1@yahoo.com

Abstract: -As information technology continues to accelerate, the need for transmitting secret information is in high demand whether information is from a corporation, the government, social media, or an individual. To meet high security and robustness requirements from various users, many steganography and cryptograph algorithms have been developed. As a result of the current advancements and developments of quantum computers and quantum computing theory, new quantum steganography schemes are more and more attractive due to their unconditional security assured by Heisenberg's uncertainty principle and no-cloning theorem. In this research, instead of using real quantum methods such as quantum key distribution (QKD, quantum secret sharing (QSS), quantum secure direct communication (QSDC), we propose a Pseudo Quantum Steganography using Pseudo Color Barcode in M-band Wavelet Domain. The probability to decode our hidden information is about $\frac{1}{2^n}$ where n is the size of that information if we perform this algorithm on a classical computer. Due to its nature, this algorithm is nearly impossible for any attackers to decode if our algorithm is performed on a quantum computer.

Key-Words: - Pseudo quantum steganography; M-band wavelets; Pseudo color barcode

1 Introduction

Steganography is a technique of hiding one piece of secret information within another, such as text, audio, image, video, and so on [4-9,16-19,21,29]. Modern steganography started during the 1980's when personal computers were affordable to general public and being applied to classical steganography problems [29]. Compared to classical cryptography, steganography can be thought as generalized cryptography using embedding techniques. The advantage of steganography is that messages can avoid causing third party's attention; therefore, it is more secure. Recent advancements in mathematical steganography theorems, quantum computing, and Big Data continue to support new algorithms, which will enforce the protection of privacy information among all users of the internet [16]. These new developments will enhance the security for electronic communication on the internet. There are many efficient steganography schemes that have been proposed.

As in [4] and [5], a secret sharing scheme is created so that an encryption key is used to encrypt the secret information that is to be securely stored/transmitted. The encrypted message is then divided into several (possibly redundant) pieces. The key is divided into shares, and these shares are stored along with the pieces of the encrypted message as an overhead

In [12], a secured robust approach of information security is proposed. The paper presents two component based LSB (Least Significant Bit) methods for embedding secret data in the LSB's of blue components and partial green components of random pixel locations on the edges of images. An adaptive LSB based steganography is proposed for embedding data based on data available in MSB's of red, green, and blue components of randomly selected pixels across smooth areas. It is more robust as it is integrated with an Advanced Encryption Standard (AES).

On the other hand, [13] provides a new high capacity stenographic scheme using 3D geometric models. The algorithm re-triangulates a part of a triangular mesh and embeds the secret information into a newly added position of triangular meshes. This algorithm also resists against uniform affine transformations such as cropping, rotation and scaling. The stego key is generated from the message to be embedded.

In [14], data is embedded into the red plane of the image, and the pixel is selected using a random number generator. It is almost impossible to notice the changes in the image. A stego key is used to seed the PRNG (Pseudo Random Number Generator) to select pixel locations. This paper focuses on increasing the security of the message and reducing the distortion rate.

Recently, more and more researchers have shifted their attentions to quantum steganography methodology due to its unconditional security.

Researchers have developed three major different quantum related steganography methods. Quantum key distribution (QKD) [1-3] is provably secure, but it remains to be made efficient in real-world applications over distances and at bit rates consistent with the requirements of modern communications. Many other quantum cryptography schemes also have been proposed and pursued, such as quantum secret sharing (QSS)[30-39], quantum secure direct communication (QSDC)[41-45], and so on. QSS is the generalization of classical secret sharing to quantum scenario and can share both classical and quantum messages among sharers. QSDC's object is to transmit the secret message directly without first establishing a key to encrypt them, which is different than QKD. QSDC can be used in some special environments, which have been shown by Boström and Deng [40].

In this research, we propose a pseudo quantum steganography within pseudo color barcode in M-band Wavelet Domain. First, we perform encryption of images, audios, text messages into a pseudo color barcode, which is tremendously useful for holding a large capacity of data due to its nature. We then perform M-band wavelet transformation to the pseudo barcode and use pseudo quantum signal transformation to encrypt our hidden information and approximation portions of the pseudo barcode. Next, we embed a hidden pseudo quantum signal into the pseudo quantum signal corresponding to approximation portions of the barcode. After the embedding, we apply the inverse wavelet transformation to get the encrypted barcode. However, the process of M-band wavelet transform, pseudo quantum transform, embedding procedure, and their inverse operations will introduce certain level of accumulated computational rounding errors and these errors can be regarded as added noise and will result in an unrecognizable decrypted signal. Thus after decryption of the secret information, we have to apply some denoising procedure to it to remove the noise. In section 4.3 we'll present our M-band wavelet package method to solve such a problem.

Our new steganography methodology has many positive outcomes such as (1) high capacity; (2) high security; (3) high imperceptibility. Assured by Heisenberg's uncertainty principle and no-cloning theorem, our algorithm is nearly impossible to any attackers to decode if our algorithm is performed on a quantum computer.

In our paper, the sections are organized as follows. Section 2 discusses the background information about the methods being used, including quantum computing, pseudo color barcode, and wavelet transformation. Section 3 describes the procedure of the steganography scheme provided with our particular example. Section 4 presents the decryption procedure including noise removal method to the extracted secret information. We will be showing some statistical results to our example in Section 5. Lastly, we state our conclusions and findings in Section 6.

2 Primaries

The following sub-sections are the background information for the methods we used to build the steganography scheme.

2.1 Quantum Computer, Qubit, and Quantum Computing

A quantum computer is a device for computations that makes direct use of quantum mechanical properties. In April of 2015, IBM researchers, for the first time, solved the key problem for building a true quantum computer: how to detect and measure both bit-flip and phase-flip quantum errors simultaneously. They also outlined a new, square quantum bit circuit design that could scale to much larger dimensions [16].

While normal computation and information are based on classical bits, quantum computation and quantum information are based on quantum bits (qubits). Just like a classical bit, either 0 or 1, a qubit also has a state. Their difference is that a qubit can be in both $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ states simultaneously and any linear combinations of them. $|0\rangle$ and $|1\rangle$are called computational basis states or basis and

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{1}$$

is called super position of $|0\rangle$ and $|1\rangle$, where a and b are complex numbers satisfying $|a|^2 + |b|^2 = 1$. Moreover, $|0\rangle$ and $|1\rangle$ form an orthonormal basis for 2-D Hilbert space, a special vector space. We can think the qubit as the following geometric representations (Fig.1), which can be rewritten as the form of qubit:

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\varphi}sin\frac{\theta}{2}|1\rangle, \tag{2}$$

where θ and φ are real numbers and a qubit defines a point on the unit 3-D sphere. Since there are infinitely many points on the unit sphere, one could store an entire set of the Shakespeare's plays in the infinite binary expansion of θ [45].

2.2 Pseudo-Quantum Signal

For the signal $S = [s_1, s_2, \ldots, s_n]^t$, we define linear transformations F so that $F(s^*) = \frac{\mathrm{m}\pi}{3}$ and $F(s_*) = \frac{m\pi}{6}$,

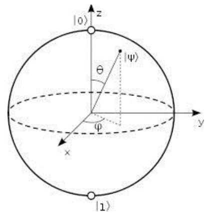


Fig. 1: Qubit

where $s^* = max\{s_k\},\ s_* = min\{s_k\}$, and $m \in \mathbb{N}$. Hence, through F we transform S into the interval $\left[\frac{m\pi}{6}, \frac{m\pi}{3}\right]$ with $\theta_k = F(s_k)$ for $k = 1,2, \ldots, n$.

We call F the "pseudo quantum signal converter" as we can transform the classical signals into the form of quantum signals through it. We now define qubit $|s_k\rangle = \cos\theta_k\, |0\rangle + \sin\theta_k\, |1\rangle$. This transform changes the signal values into the form of angles, thus we can define corresponding qubits to represent the signal.

Definition: The corresponding qubits $|\, s_k \rangle = \cos\theta_k\, |0\rangle + \sin\theta_k\, |1\rangle|$ are called pseudo quantum signals.

After all, they are not exactly the same as real quantum signals, so we call them "pseudo quantum signals". This can help us simulate quantum signals and quantum computing in situations where quantum computers are not available.

2.3 Pseudo Color Barcode

Barcodes are optical machine-readable signals of data, that are capable of storing digital information about the physical object to which they are attached. Both the increasing demand for higher density barcodes and the wide availability of on-board cameras in mobile phones naturally seem to motivate the need for 2-D color barcodes. In this research, we do not use the real color barcode; instead, we convert the three pieces of host signals into an image that looks like a color barcode with three different color channels. This pseudo color barcode can hold three books such as three volumes of *The Lord of the Rings*. We then embed our secret information into this "barcode".

2.4 M-Band Wavelet

Discrete M-Band Wavelet Transform uses a set of M filter banks ($M \geq 2$) to break a k dimensional signal into M^k different frequency levels. Daubechies wavelets are classical 2-Band wavelets.

A 4-Band 2-D wavelet transform decomposes an image into one approximation (low frequency) component and 15 detail (high frequency) components. The 2-D discrete M-Band wavelet transformation of an image matrix I is done by multiplying a wavelet transform matrix to the left side of input image and then by its transpose to the right side, written as TIT^t, where T is the wavelet transform matrix, which is orthonormal, and T^t is the transpose of T and hence $T^t = T^{-1}$.

In order to apply DMWT to a color image, we decompose the RGB-mode color image into three matrices, I_1, I_2, and I_3 for red, green, and blue, respectively. We then apply DMWT to each one of them to obtain

$$I'_k = T I_k T^t \tag{3}$$

for $k = 1,2,3$, respectively. Therefore, the transformed image can be formed by the combination of I'_1, I'_2, and I'_3. An example of 4-band wavelet transform matrix T is given below:

$$T = \begin{bmatrix}
v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \\
v_5 & v_6 & v_7 & v_8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_1 & v_2 & v_3 & v_4 \\
w_1^{(1)} & w_2^{(1)} & w_3^{(1)} & w_4^{(1)} & w_5^{(1)} & w_6^{(1)} & w_7^{(1)} & w_8^{(1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & w_1^{(1)} & w_2^{(1)} & w_3^{(1)} & w_4^{(1)} & w_5^{(1)} & w_6^{(1)} & w_7^{(1)} & w_8^{(1)} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w_1^{(1)} & w_2^{(1)} & w_3^{(1)} & w_4^{(1)} & w_5^{(1)} & w_6^{(1)} & w_7^{(1)} & w_8^{(1)} \\
w_5^{(1)} & w_6^{(1)} & w_7^{(1)} & w_8^{(1)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w_1^{(1)} & w_2^{(1)} & w_3^{(1)} & w_4^{(1)} \\
w_1^{(2)} & w_2^{(2)} & w_3^{(2)} & w_4^{(2)} & w_5^{(2)} & w_6^{(2)} & w_7^{(2)} & w_8^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & w_1^{(2)} & w_2^{(2)} & w_3^{(2)} & w_4^{(2)} & w_5^{(2)} & w_6^{(2)} & w_7^{(2)} & w_8^{(2)} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w_1^{(2)} & w_2^{(2)} & w_3^{(2)} & w_4^{(2)} & w_5^{(2)} & w_6^{(2)} & w_7^{(2)} & w_8^{(2)} \\
w_5^{(2)} & w_6^{(2)} & w_7^{(2)} & w_8^{(2)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w_1^{(2)} & w_2^{(2)} & w_2^{(3)} & w_2^{(4)} \\
w_1^{(3)} & w_2^{(3)} & w_3^{(3)} & w_4^{(3)} & w_5^{(3)} & w_6^{(3)} & w_7^{(3)} & w_8^{(3)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & w_1^{(3)} & w_2^{(3)} & w_3^{(3)} & w_4^{(3)} & w_5^{(3)} & w_6^{(3)} & w_7^{(3)} & w_8^{(3)} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w_1^{(3)} & w_2^{(3)} & w_3^{(3)} & w_4^{(3)} & w_5^{(3)} & w_6^{(3)} & w_7^{(3)} & w_8^{(3)} \\
w_5^{(3)} & w_6^{(3)} & w_7^{(3)} & w_8^{(3)} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & w_1^{(3)} & w_2^{(3)} & w_3^{(3)} & w_4^{(3)}
\end{bmatrix}$$

where:

v= [-0.06737176, 0.09419511, 0.40580489, 0.56737176, 0.56737176, 0.40580489, 0.09419511, -0.06737176]

$w^{(1)}$= [-0.09419511, 0.06737176, 0.56737176, 0.40580489, -0.40580489, -0.56737176, -0.06737176, 0.09419511]

$w^{(2)}$= [-0.09419511, -0.06737176, 0.56737176, -0.40580489, -0.40580489, 0.56737176, -0.06737176, -0.09419511]

$w^{(3)}$= [-0.06737176, -0.09419511, 0.40580489, -0.56737176, 0.56737176, -0.40580489, 0.09419511, 0.06737176].

It's easy to verify that

$$\sum_{i=1}^{8} v_i = \sqrt{4} = 2, \sum_{i=1}^{8} w_i^{(1)} = \sum_{i=1}^{8} w_i^{(2)} = \sum_{i=1}^{8} w_i^{(3)} = 0,$$

$$\|\boldsymbol{v}\| = \|w^{(1)}\| = \|w^{(2)}\| = \|w^{(3)}\| = 1,$$

$$\boldsymbol{v} \cdot w^{(1)} = \boldsymbol{v} \cdot w^{(2)} = \boldsymbol{v} \cdot w^{(3)} = w^{(1)} \cdot w^{(2)} = w^{(1)} \cdot w^{(3)} = w^{(2)} \cdot w^{(3)} = 0 \qquad (4)$$

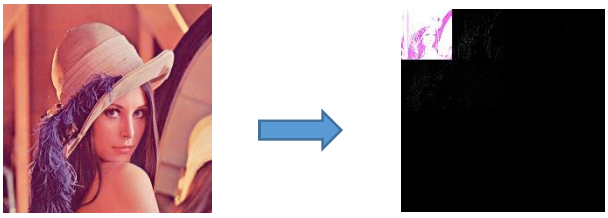


Fig. 2 Original image and its corresponding wavelet transformed image. In the right picture, left top part is approximation; other parts are details.

3 Steganography procedure

The steganography algorithm consists of the following seven sub-sections.

3.1 Convert the host information into pseudo barcodes

Each alphabet and the special characters correspond to an American Standard for Information Interchange (ACSII) code. For example, "a" corresponds to number 63, "b" corresponds to number 64, "c" corresponds to number 65, "period/(.)" corresponds to number 46, "comma/(,)" corresponds to number 44, etcetera. We convert the entire host message into a sequence of ASCII numbers and then reshape them into a square matrix. If the message does not completely fill the square matrix, we insert extra "spaces" to fill it. "Space" corresponds to number 32 in ASCII format.

In our example, we are using true color (RGB) barcode, so it consists of three color channels: red, green, and blue. Therefore, we can have up to three host messages corresponding to each color channel and up to three types of secret information to be embedded in corresponding host messages.

Text secret information will be converted and reshaped into the square matrix using a similar method as the host messages. Image secret information will be converted into greyscale. Then, we use MATLAB to get the corresponding color intensity at each pixel. Audio secret information will be digitalized and reshaped into square matrix. The size of the secret information is one-sixteenth to the host message since we will embed the secret information into the approximation portion of the host message. Approximation portion is the results of M-Band Wavelet Transformation, which will be presented in 3.2.

Each host message channel is in greyscale, and the color intensity has a bound of 0-255. By combining three grayscale images, we obtain a RGB color image. Call each image R, G, B respectively.

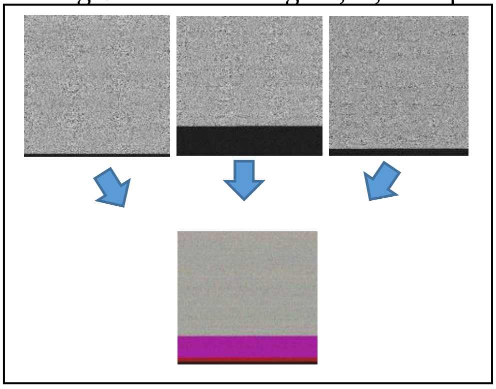


Fig. 3: The Lord of The Rings books in the "color barcode"

3.2 M-Band Wavelet Transformation

As in the description of M-Band Wavelet in sub-section 2.4 from Section 2, by performing M-Band Wavelet transformation, we get the approximation portion, which contains the most energy of the host message (as seen in Fig. 4. Because we are using 4-Band Wavelet, the approximation portion is one-sixteenth the size of the barcode. We want to encrypt the secret information into these approximation portions. Therefore, the size of the secret information must match the size of the approximation portion. We call each transformed matrix WR, WG, WB.

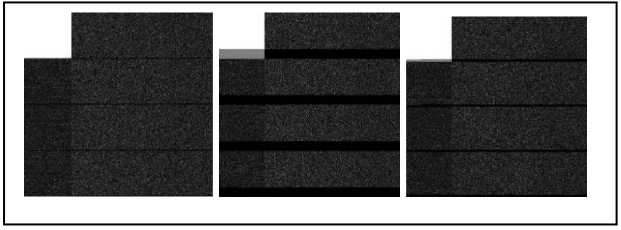


Fig. 4: Post Wavelet Transformation on host information

3.3 Secret Information

We want to embed the secret information into the approximation portion of the host channels. Secret information can be in the form of text, image, and audio. We call these pieces of secret information *X*, *Y*, and *Z*, respectively. The ways to digitalize the secret information has been mentioned in sub-section 3.1.

3.3.1 Texture*:*

If the host message has the size of 1024 x 1024, then the text secret information can get up to 65536 characters (approximate 9000 words).

3.3.2 Image*:*

Any grayscale image with the size of the approximation portion of the host image.

3.3.1 Audio:

We use MATLAB to break down audio index and reshape it into a square matrix with the same size as other secret information.

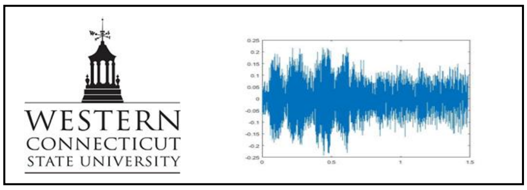


Fig. 5: Image and audio secret information

3.4 Angle Transformation

In order to perform quantum encryption, which has been introduced in sub-sections 2.1, 2.2, and 2.3, the host and the secret information must be in the form of an angle. For encryption, we only encrypt the secret information to the approximation portion. Therefore, we only take the approximation portions, called matrix A_R, from the matrix W_R, and transform it into angle element in the interval $[\frac{m\pi}{6}, \frac{m\pi}{3}]$ using the following operation f.

Let $\mu_1 = \max(A_{(R,ij)}), \nu_1 = \min(A_{(R,ij)})$. We acquire:

$$\theta_{R,ij} = f(A_{R,ij}) = \frac{m\pi(A_{R,ij} + \mu_1 - 2\nu_1)}{6(\mu_1 - \nu_1)}. \quad (5)$$

And denote $\theta_R = [\theta_{R,ij}]$.

Then, we perform the same operation to the secret information X in the interval of $[\frac{n\pi}{6}, \frac{n\pi}{3}]$

Let $\mu_2 = \max(X_{ij}), \nu_2 = \min(X_{ij})$. We acquire:

$$\alpha_{ij} = f(X_{ij}) = \frac{n\pi(X_{ij} + \mu_2 - 2\nu_2)}{6(\mu_2 - \nu_2)} \quad (6)$$

Let: $\alpha = [\alpha_{ij}]$

Perform the procedure of sub-section 3.4 for matrices W_G, W_B, Y, and Z to obtain $\theta_G, \theta_B, \beta, \gamma$ respectively; then, save all the maximum and minimum values into codebooks.

3.5 Random Qubit

For each pixel (i,j) if we have a quantum computer, then we can get a random qubit

$$|k_{ij}\rangle = P_{ij_1}|0\rangle + P_{ij_2}|1\rangle \quad (7)$$

Since we are performing the transformation on a classical computer, we cannot generate a true quantum qubit. Therefore, we applied the random number generator to represent the randomness of quantum qubit.

$$k_{ij} = rand(0,1) \quad (8)$$

k_{ij} is the random number between 0 and 1. We generate *K* for each pixel of the matrix.

3.6 Embedding Using Quantum/Pseudo Quantum Signals

For quantum signal:

$$\theta_{ER,ij} = m\begin{cases} \cos^{-1}(\cos(\frac{\theta_{R,ij}}{m}) + \varepsilon\cos(\frac{\alpha_{ij}}{n})), & |P_{ij1}| \geq |P_{ij2}| \\ \sin^{-1}(\sin(\frac{\theta_{R,ij}}{m}) + \varepsilon\sin(\frac{\alpha_{ij}}{n})), & |P_{ij_1}| < |P_{ij2}| \end{cases} \quad (9)$$

Let: $\theta_{ER} = [\theta_{ER,ij}]$

For pseudo quantum signal:

$$\theta_{ER,ij} = m\begin{cases} \cos^{-1}(\cos(\frac{\theta_{R,ij}}{m}) + \varepsilon\cos(\frac{\alpha_{ij}}{n})), & k_{ij} \geq 0.5 \\ \sin^{-1}(\sin(\frac{\theta_{R,ij}}{m}) + \varepsilon\sin(\frac{\alpha_{ij}}{n})), & k_{ij} < 0.5 \end{cases} \quad (10)$$

We perform the similar procedure to the θ_G, θ_B to obtain θ_{EG}, θ_{EB}. To get the encrypted approximation portion, we perform the inverse of transformation of (5).

$$A_{WR,ij} = \frac{6\theta_{ER,ij}(\mu_1 - \nu_{1)}}{m\pi} - \mu_1 + 2\nu_1 \quad (11)$$

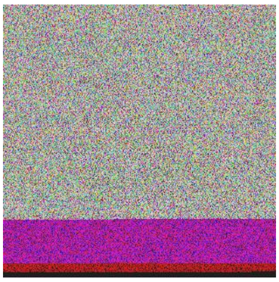
Let $A_{WR} = [A_{WR,ij}]$. A_{WR} is the encrypted approximation portion for the red channel.

Perform the same operation for the approximation portion of the green and blue channel.

Note: Unlike image and audio secret information, text secret information is difficult to decrypt due to rounding error. For image and audio secret information, a human can recognize the image and sound if they are similar to each other (see Statistical Result). However, for text secret information, we have not yet achieved 100% similarity. Therefore, in order to decrypt the message, we have to save the rounding error to the code book and add it back during the decryption step.

3.7 Embedded Barcode

Now, we replace the encrypted approximation portion to the wavelet transformed host matrix. Call these new matrices W_{ER}, $W_{EG,}$ W_{EB}. Then, we perform the inverse wavelet transformation to these matrices to obtain the encrypted host message.



$$\begin{aligned} R_E &= T^{-1} W_{ER} T \\ G_E &= T^{-1} W_{EG} T \\ B_E &= T^{-1} W_{EB} T \end{aligned} \qquad (12)$$

Fig. 6: Encrypted Barcode

4 Decryption

4.1 Obtain the encrypted approximation portions

After the receiver obtains the original and the encrypted barcodes along with the code book, he/she needs to perform the same procedures of sub-sections 3.2 and 3.4 from Section 3 to get into the encrypted approximation portions of each channel in angle form. From the procedure, the receiver will obtain $\theta_{R,ij}, \theta_{G,ij}, \theta_{B,ij}$ from the original barcode and $\theta_{ER,ij}, \theta_{EG,ij}, \theta_{EB,ij}$ from the encrypted ones.

4.2 Decrypt secret information

For quantum signal:

$$\alpha_{ij} = n \begin{cases} \cos^{-1}\left(\dfrac{\cos(\frac{\theta_{ER,ij}}{m}) - \cos(\frac{\theta_{R,ij}}{m})}{\varepsilon}\right), & \left|P_{ij_1}\right| \geq \left|P_{ij_2}\right| \\ \sin^{-1}\left(\dfrac{\sin(\frac{\theta_{ER,ij}}{m}) - \sin(\frac{\theta_{R,ij}}{m})}{\varepsilon}\right), & \left|P_{ij_1}\right| < \left|P_{ij_2}\right| \end{cases} \qquad (13)$$

For pseudo-quantum signal:

$$\alpha_{ij} = n \begin{cases} \cos^{-1}\left(\dfrac{\cos(\frac{\theta_{ER,ij}}{m}) - \cos(\frac{\theta_{R,ij}}{m})}{\varepsilon}\right), & k_{ij} \geq 0.5 \\ \sin^{-1}\left(\dfrac{\sin(\frac{\theta_{ER,ij}}{m}) - \sin(\frac{\theta_{R,ij}}{m})}{\varepsilon}\right), & k_{ij} < 0.5 \end{cases} \qquad (14)$$

Perform the same operation to obtain β and γ .

Remember that α is the secret information embedded into the red channel, β is the secret information for the green channel, and γ is the audio secret information for the blue channel.

However, α, β, and γ are in the angle form due to the transformation from sub-section 3.4. Therefore, we need to perform the inverse linear transformation to get back to the original signal.

$$X^*_{ij} = \frac{6\alpha_{ij}(\mu_2 - \nu_2)}{n\pi} - \mu_2 + 2\nu_2 \qquad (15)$$

We perform the same transformation for β and γ to get $Y*$ and $Z*$. If there were absolutely no rounding errors during computations involved in our steganography progress, we would obtain exactly *X*, *Y*, and *Z* by (15). For $Z*$(audio secret information), we need to reshape back to get the audio form that was performed in sub-section 3.3.1.

4.3 Noise Removal

The process of M-band wavelet transform, pseudo quantum transform, embedding procedure, and their inverse operations will introduce a certain level of accumulated rounding errors. We can regard theses accumulated rounding errors as added noise. Thus, when a receiver applies the steps as in sub-sections 4.1 and 4.2 to decrypt the secret information, he/she inevitably obtains the corresponding information with added noise. If the noise is heavy, it may affect the receiver to correctly read the information, he/she decrypted from the embedded pseudo barcode sent to him/her. Therefore, it's necessary for us to develop and apply a denoising algorithm to decrypted secret information to remove corresponding noise.

Suppose we apply decryption procedure described in 4.1 and 4.2 to obtain $X^*_{.}$ $Y^*_{,}$and $Z^*_{.}$ Then

$$\begin{cases} X^* = X + n_x^{\cdot} \\ Y^* = Y + n_y \\ Z^* = Z + n_z \end{cases} \qquad (16)$$

where $n_x, n_y,$ and n_z are noise contained in $X^*, Y,^*$ and Z^*.

To remove the noise, we employ wavelet denoising technics. These techniques utilize wavelet transform, which concentrates secret information features into a few large magnitude wavelet coefficients. The smaller wavelet coefficients are likely to be noise that can be either diminished or removed without affecting the signal’s quality. Wavelet transform decomposes a 2-D signal into one lower frequency subband (approximation portion) that contains most of the signal’s information and energy and high frequency subbands (details) that contain most of the noise information.

The following sub-sections will show how our algorithm works. We apply 4-band wavelet transform to $X^*, Y^*,$ and $Z^* \in \mathbb{R}^{4^n \times 4^n}$, respectively, resulting in one approximation (A) and 15 details (D$_1$,D$_2$, … , D$_{15}$) for each one of .them. We then perform 4-band wavelet transform to the fifteen $4^{n-1} \times 4^{n-1}$ details, separating each of them into sixteen $4^{n-2} \times 4^{n-2}$.portions (D$_i$’s approximations and 15 details for i =1,…,15). Let A_i be the approximation and D_{ij} be the details of D_i for $i, j = 1, \dots, 15$. After doing so, we set a local hard threshold $T_{ij} = \sigma_{ij}\sqrt{2logK}$ on each of the D_{ij} and $\Psi_i = \Sigma_i \sqrt{\log K}$ on each of $A_i$for i, j=1,…,15 and K =4^{n-1} to remove noise where σ_{ij}'s and $\Sigma_i's$ are the standard deviations of D_{ij} and A_i, respectively.

4.4 Decryption Results

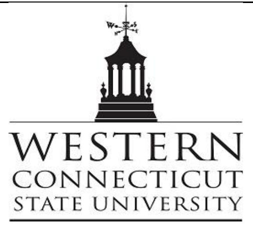
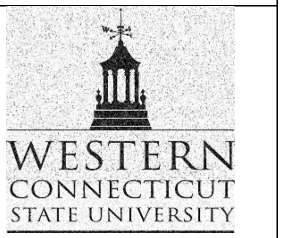
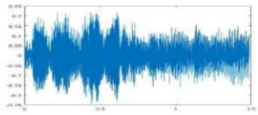
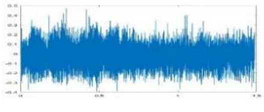
Original secret information	Decrypted Secret information
The film begins with a summary of the prehistory of the ring of power…	The film begins with a summary of the prehistory of the ring of power…
	
	

Fig. 7: Comparison of the original secret information and the decrypted secret information

5 Statistical Results

To measure the quality, security, and robustness of embedded information and to compare the similarity between the host information and the embedded information, we use the following algorithms.

Given a noise-free $m \times n$ image (host barcode) I and its noisy approximation K (Encrypted barcode), MSE (Mean Square Error) is defined as:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(I_{ij} - K_{ij})^2 . \qquad (17)$$

Then, the Peak Signal-to-Noise Ratio is defined and denoted as

$$PSNR = 10 \cdot \log(\frac{255^2}{MSE}) . \qquad (18)$$

Normally, the higher PSNR means the better quality of encrypted “color barcodes”.

For images (barcodes) I_1 and I_2, the relative similarity (RS) of I_2 to I_1 is defined by

$$RS(I_2, I_1) = 1 - \frac{\left\|I_2 - I_1\right\|_1}{\left\|I_1\right\|_1} , \qquad (19)$$

where $||A||_1$ is the 1-norm of matrix A.

The following table shows the PSNR and RS for encrypted “color barcodes” with different embedding intensity and parameters m and n.

		n=6, m=6		n=12, m=12	
Channel	ε	PSNR	RS	PSNR	RS
Red	.003	48.05	.9939	48.04	.9939
	.005	43.85	.9902	43.83	.9901
	.01	37.91	.9805	37.89	.9805
	.02	31.86	.9609	31.85	.9608
Green	.003	47.87	.9932	47.88	.9932
	.005	43.67	.9843	43.68	.9890
	.01	37.78	.9782	37.76	.9782
	.02	31.69	.9561	31.70	.9562
Blue	.003	46.18	.9923	46.17	.9882
	.005	41.88	.9874	41.88	.9874
	.01	35.87	.9749	35.86	.9748
	.02	29.81	.9495	29.81	.9495

		n=6, m=6		n=12, m=12	
Secret	ε	PSNR	RS	PSNR	RS
	Before Denoise				
Image	.003	10.65	.6867	10.69	.6884
	.005	14.25	.7932	14.44	.7977
	.01	21.48	.9096	21.45	.9093
	.02	30.20	.9668	30.19	.9668
	After Denoise				
	.003	20.22	.8563	20.25	.8574
	.005	24.31	.9161	24.32	.9268

	.01	29.16	.9515	29.24	.9556
	.02	37.47	.9813	37.48	.9813

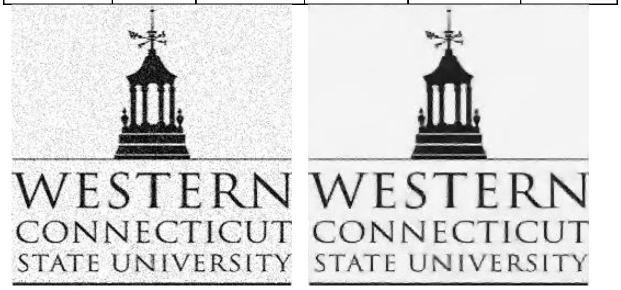


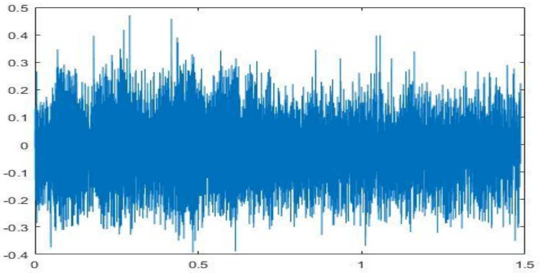
Fig. 8: Comparison of the extracted and denoised image secret using ε=.005

To compare the original and the extracted audio secret information, we use a different algorithm called Signal to Noise Ratio:

$$SNR = 10\log\left\{\frac{\sum_{a=1}^{M_t} Z^2(a)}{\sum [Z(a) - Z*(a)]^2}\right\} \quad (20)$$

where Z is the original audio signal, and Z* is the extracted audio signal. As the difference between the original signal and the extracted signal is small, we are expected to get a bigger ratio since we are dividing by a small denominator. In our sample, at ε =.005, we are getting an extracted audio with noises. However, it is clear enough for the audience to receive the audio message.

		n=6, m=6	n=12, m=12
Secret	ε	SNR	SNR
	Before Denoise		
Audio	.005	5.76	5.73
	.01	19.57	19.49
	.02	39.44	39.33
	.1	75.34	75.32
	After Denoise		
	.005	19.46	17.10
	.01	34.99	35.00
	.02	52.82	52.64
	.1	64.15	64.11



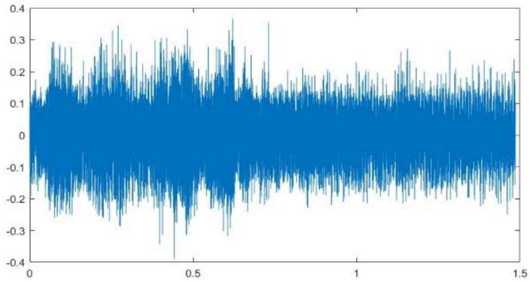


Fig. 9: Comparison of the extracted and denoised audio secret using ε=.005

6 Conclusion and future research

In this paper, we present a new pseudo quantum steganography with “Color Barcode” in M-band Wavelet Domain. We have shown the efficiency and security in applying our method for performing encryption of our hidden information. As a result, the encrypted “color barcodes” with such a well-chosen embedding domain is much safer and more difficult to attack. This algorithm can be carried out on both classical computers and quantum computers, so it can be widely used for audio, video, and still image file’s encryption and security information transmission, etc. Assured by Heisenberg’s uncertainty principle and no-cloning theorem, this algorithm is nearly impossible for any attackers to decode if our algorithm is performed on a quantum computer.

In our future research, we will derive a true color barcode based Pseudo Quantum Steganography algorithm, which will hold more information. Moreover, it will be more convenient for receivers to decode while more difficult for attackers to defeat.

7 Acknowledgement

We are grateful to SGA of Western Connecticut State University for the financial support. Special thanks to Department of Math and School of Arts & Science at Western Connecticut University for their academic support and constant encouragement.
Special thanks to Mrs. Stacey Brugnolo at Danbury High School for proof reading this research paper.

References:

[1] C. H. Bennett and G. Brassard. Quantum cryptography. “Public key distribution and coin tossing”. In Proceedings of IEEE International Conference on Computers Systems and Signal Processing, volume 175, page 8. New York, 1984.

[2] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, "Decoy State Quantum Key Distribution" Physical Review Letters, 94, 230504 (2005)

[3] C. Gobby,a Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber”, Applied Physics Letters 84, 3762-3764(2004).

[4] P. Rogaway and M. Bellare, “Robust computational secret sharing and a unified account of classical secret-sharing goals,” in CCS ’07: Proceedings of the 14th ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 2007, pp. 172–184.

[5] H. Krawczyk, “Secret sharing made short,” Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, pp. 136–146, 1994.

[6] T. Zhang and X. Ping, “A New Approach to Reliable Detection of LSB Steganography in Natural Images”, Signal Processing, vol. 83, No. 10, pp. 2085–2094, 2003.

[7] J. Fridrich and M. Goljan, “On Estimation of Secret information Length in LSB Steganography in Spatial Domain”, to appear in EI SPIE Electronic Imaging, San Jose, January 18–22, 2004.

[8] Jiufen LIU, Yuguo TIAN1, Tao HAN1, Junchao WANG, Xiangyang LUO, “Stego key searching for LSB steganography on JPEG decompressed image”, SCIENCE CHINA Information Sciences, Vol. 59 Issue: 032105,2015.

[9] R.J. Anderson and F.A.P. Petitcolas, “On the Limits of Steganography”, IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection, vol. 16(4), pp. 474−481, 1998.

[10] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB Steganography in Color and Gray-Scale Images”, *Magazine of IEEE Multimedia, Special Issue on Security*, October-November issue, pp. 22–28, 2001.

[11] Mamta Juneja and Parvinder Singh Sandhu, (2013) “A New Approach for Information security using an Improved Steganography Technique”, Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.

[12] P.Thiyagarajan, V.Natarajan, G.Aghila, V.Pranna Venkatesan, R.Anitha, (2013) “Pattern Based 3D Image Steganography”, 3D Research center, Kwangwoon University and Springer 2013, 3DR Express., pp.1-8.

[13] Shamim Ahmed Laskar and Kattamanchi Hemachandran, (2013) “Steganography Based On Random Pixel Selection For Efficient Data Hiding”, International Journal of Computer Engineering and Technology, Vol.4, Issue 2, pp.31-44.

[14] S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) “Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain”, International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp. 2632-2637.

[15] C.P.Sumath, T.Santanam and G.Umamaheswar, (2013), “A Study of Various Steganographic Techniques Used for Information Hiding”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6.

[16] Akbas E. Ali (2010). "A New Text Steganography Method By Using Non-Printing Unicode Characters". Eng. & Tech. Journal 28 (1).

[17] Steven J. Murdoch and Stephen Lewis (2005). "Embedding Covert Channels into TCP/IP". Information Hiding Workshop.

[18] Krzysztof Szczypiorski (October 2003). "HICCUPS: Hidden Communication System for Corrupted Networks". In Proc. of: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003, pp. 31-40.

[19] Tong Liu, Xuan Xu, Xiaodi Wang, “M-band Wavelet Based Pseudo Quantum Watermarking”, The 2nd International Conference of Mathematics and Computers in Sciences and Industry-MSCI2015, Sliema, Malta, August 17-19, 2015.

[20] Tong Liu, Xuan Xu, Xiaodi Wang, “M-band Wavelet and Cosine Transform Based Watermark Algorithm Using Randomization and Principle Component Analysis”, International Journal of Science and Engineering Investigations, vol. 2, issue 13, pp. 1-4, February 2013.

[21] Gary C. Kessler, “Steganography: Hiding Data Within Data”, 2001

[22] Takashi Mihara “Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data”, Journal of Quantum Information Science, 2012, 2, 10-14

[23] Bilal A. Shaw and Todd A. Brun “ Quantum steganography with noisy quantum channels”, Phys. Rev. A 83, 022310 – Published 14 February 2011

[24] Zhan-Hong Wei, Xiu-Bo Chen , Xin-Xin Niu, Yi-Xian Yang ” The Quantum Steganography Protocol via Quantum Noisy Channels”, International Journal of Theoretical Physics, August 2015, Volume 54, Issue 8, pp 2505-2515

[25] Zhanhong Wei “A Novel Quantum Steganography Protocol Based on Probability Measurements”, International Journal of Quantum Information, Volume 11, Issue 07, October 2013

[26] Xu, Shujiang; Chen, Xiubo; Niu, Xinxin; Yang, Yixian “Steganalysis and improvement of a quantum steganography protocol via a GHZ4 state”, Chinese Physics B, Volume 22, Issue 6, 2013.

[27] Takashi Mihara “Quantum steganography using prior entanglement”, Physics Letters A, Volume 379, Issues 12–13, 5 June 2015, Pages 952–955.

[28] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, “Information Hiding-A Survey”, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062-1078, July 1999.

[29] A. Karlsson, M. Koashi, and N. Imoto, “Quantum entanglement for secret sharing and secret splitting”, Phys. Rev. A 59, 162 (1999).

[30] Z. J. Zhang, Phys. Lett. A 342, 60 (2005).

[31] G. P. Guo and G. C. Guo, Phys. Lett. A 310, 247 (2003).

[32] Z.J. Zhang, Yong Li, and Zhong-xiao Man, Phys.
Rev. A 71, 044301 (2005).

[33] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan, Phys. Rev. A 69, 052307 (2004)

[34] Z. J. Zhang, Z. X. Man, Phys. Rev. A 72 (2005) 022303.

[35] J. Wang, Q. Zhang, C. J. Tang, Commun. Theor. Phys. 47 (2007).

[36] S. Lin, F. Goa, F. Z. Guo, Q. Y. Wen, F.C. Zhu, Phys. Rev. A 76 (2007) 036301.

[37] .C. R. Hsieh, C. W. Tasi, T. Hwang, Commun. Theor. Phys. 54 (2010) 1019. [30].

[38] X. B. Chen, X. X. Niu, X. J. Zhou, Y. X. Yang, Quantum Inf. Process. 12 (2013) 365.

[39] A. Beige, B. G. Engler, C. Kurtsiefer, H. Weinfurter, Acta Phys. Pol. A 101 (2002) 357.

[40] F. G. Deng, G. L. Long, Phys. Rev. A 69 (2004) 052319.

[41] J. Wang, Q. Zhang, C. J Tang, Phys. Lett. A 358 (2006) 256.

[42] T. Gao, F. Yan, Zh. Wang, arXiv:0406083v1 [quant-ph].

[43] K. Li, X. Y. Huang, J. H. Teng , Z. H. Li, Third International Conference on Multimedia Information Networking and Security, 2011, p.73.

[44] K. Boström, T. Felbinger, Phys. Rev. Lett. 89 (2002) 187902.

[45] A. Wójcik, Phys. Rev. Lett. 90 (2003) 157901.