GOLDEN RATIO-HAAR WAVELET BASED STEGANOGRAPHY

Sos S. Agaian\textsuperscript{1}, Okan Caglayan\textsuperscript{1}, Juan Pablo Perez\textsuperscript{1}, Hakob Sarukhanyan\textsuperscript{2}, Jaakko Astola\textsuperscript{3}

\begin{itemize}
\item \textsuperscript{1}Multimedia and Mobile Signal Processing Laboratory, University of Texas San Antonio, San Antonio, TX, USA, sagaian@utsa.edu, ocaglayan@lonestar.utsa.edu, jpperez@lonestar.utsa.edu
\item \textsuperscript{2}Institute for Informatics and Automation Problems of NAS of Armenia, hakop@ipia.sci.am
\item \textsuperscript{3}Tampere International Center on Signal Processing, Tampere University of Technology, Tampere, Finland, jta@cs.tut.fi
\end{itemize}

\section*{ABSTRACT}

In this paper, we have presented the golden ratio-Haar wavelet based multimedia steganography. The key features of the proposed method are:

1. New Haar wavelet structure based on the Fibonacci sequence, and Golden Ratio.
2. Parametric transform dependency, as decryption key, on the security of the sensitive data.

One of the important differences between the existing transform based data hiding techniques and the proposed is that not only the pseudo-random keys provided by the data hiding methods are vital, but also the parametric transform we proposed, which has become a key, is necessary in order to reconstruct the secret message.

\section{INTRODUCTION}

The rapid growth of multimedia processing technologies and the wide range of network access availability have enabled many powerful and creative applications. Digital multimedia data, such as digital images, audio, video, and documents, can be created, edited, distributed, shared, and stored with convenience at a very low cost, e.g. on the Internet. On one hand, new technologies help individuals to achieve better communications with one another. On the other hand, since the emerging Internet is an open network which is vulnerable to eavesdropping or unauthorized users, the fear that the multimedia data transmitted through the Internet could be manipulated or stolen is inhibiting the progress of multimedia Internet applications [5].

Authentication control mechanisms can be used to secure distributed multimedia applications. However, it is not enough to secure vital data during the broadcast on the open networks, such as Internet, wireless networks. Cryptography (encryption) provides the tools to secure the sensitive data, by encrypting it into a manner which is not discernible to an attacker without the secret key [14]. On the other hand, steganography (data hiding) is the secure communication of information by embedding a message into a ‘cover’ digital media in a manner that is undetectable by external observers. The message may at any time be retrieved from the transmitted/stored digital media file. Data hiding has been proposed as a promising approach for the purpose of information assurance, authentication, fingerprint, security, data mining, and copyright protection, etc. [15].

Multimedia steganography has applications in the internet communication, multimedia database systems, medical imaging, telemedicine, and military communications [1]. The challenges of the multimedia data security arise when a malicious opponent applied various data processing operations to interfere with decoder’s ability to recover the hidden data. In other applications, there might not be an unauthorized user, but manipulations of the modified data set might result in similar unfortunate effects. Therefore, the problem of providing secure image steganography technology has been and endures as a problem of prime concern.

Recently, a number of time-frequency domain based algorithms have been presented to maintain the confidentiality and the integrity of the vital information. I.J.Cox et al. [8] developed a data hiding algorithm that added the scaled and transformed secured information into low frequency coefficients of the cover image. Miyazaki et al. [26] proposed a new multi-channel robust watermarking based on a diversity technique for color images. Satish et al. [29] introduced a chaos based spread spectrum image steganography (CSSIS) method. The CSSIS is inexpensive to produce, and can be used for ensuring security and privacy. Robustness is achieved by interleaving the message using a chaotic sequence. Agaian and Cherukuri [28] proposed a multiband concept based data hiding procedure offering a higher level of security. The various energy coefficients of stego are scaled using a varying scaling factor thus making the embedded information more robust to ordinary image processing operations.

This paper presents the new parametric Haar wavelet based on the Golden Ratio structure. Furthermore, we have shown the application point of this proposed transform in the image steganography. In the proposed steganographic method, the parametric Haar transform has become an important feature in order not only to embed the data securely, but also retrieve it based on the parametric key.

The rest of the paper is organized as the following. Section II briefly describes the steganography and golden Fibonacci transform; Section III discusses the proposed system; Section IV has shown the experimental results; Conclusion is drawn in section V.

\section{BACKGROUND}

In this section, we briefly discuss the steganography, and Golden Ratio Fibonacci transforms.

\subsection{Steganography}

In recent years, steganography has become a very popular means for securing data. Modern steganography is the secure communication of information by embedding a sensi
ative message within a digital multimedia file, known as the cover, without any perceptible distortion of the cover media so that the presence of the hidden message is indiscernible. The medium which is to be used as the carrier of an embedded message is referred to as the cover-medium. The combined signal, which is the cover-medium with message inserted, is usually referred to as the stego-medium. Figure 1 has shown an illustrative example of existing steganographic techniques for the multimedia data security.

![Figure 1: Block diagram of the commonly used steganographic techniques.](image)

Steganography not only provides a procedure for transmitting a secret message which disallows others from having access to what is sent, but it also conceals the presence of any actual communication [1]. The actual process of data embedding depends on the nature of the cover media. The cover media can be pictures, videos, music, text, a source code file, ciphertext, and can also be created synthetically. These data formats have potential for information hiding due to the redundancy and irrelevancy inherent in digital media. For example, the validity of a digital image as cover medium is justified when considering the limitations of the human visual system (HVS) and a cover image: 3135x2295 bmp, 24 bit/pixel, 7 MB, which has an embeddable data capacity of approximately 2.2 MB. The primary goals of steganographic systems are a) to hide information in ways that are both perceptually and statistically undetectable; and b) to achieve high security and high capacity [1].

### 2.2. Golden Fibonacci Transforms

Golden Fibonacci sequences are a generalization of Fibonacci sequences, and the related Golden Fibonacci transforms are a generalization of the Fibonacci transforms. In this section, we have briefly discussed the properties of Fibonacci sequences, Golden Fibonacci transform, and have given basic definitions, notations used in the theory of Golden Fibonacci transform, and shown illustrative examples.

Discrete orthogonal transforms in terms of Fibonacci sequences are introduced in [2]. Fast algorithms for their computation were discussed in [3]. These methods permit to process by generalized Fibonacci transforms functions defined in a large number of points, which overcome the limitations of algorithms related to their exponential complexity in both space and time.

The Fibonacci transform is defined by referring to the Fibonacci sequence, that is defined as a sequence of numbers $\phi(i)$, where $\phi(0) = 1$, $\phi(i) = 0$ for $i < 0$ and

$$
\phi(i) = \phi(i-1) + \phi(i-2), \quad i > 0.
$$

The generalized Fibonacci transforms are defined by referring to the generalized Fibonacci sequences by

$$
\phi_p(i) = \begin{cases} 0, & i < 0, \\
1, & i = 0, \\
\phi_p(i - 1) + \phi_p(i - p - 1), & i > 0.
\end{cases}
$$

Golden Fibonacci transform is a generalization of the Fibonacci transform and also relates to the generalized Fibonacci transforms. It is derived by referring to the golden Fibonacci sequence defined by the requirement

$$
\phi^i = \phi^{i-1} + \phi^{i-2}
$$

for $i \geq 2$, where $\phi$ is the golden ratio defined in terms of golden section $\tau$, thus, $\phi = \tau^{-1}$.

**Golden Fibonacci Transform:** We have built the following $4 \times 4$ matrix with pairwise orthogonal rows in order to illustrate the straightforward generalizations to the matrices of higher orders [1]

$$
Z_4 = \begin{bmatrix}
1 - \tau^{-1} & 0 & 0 & 0 \\
1 - \tau^{-2} & \tau^{-1} & 0 & 0 \\
1 & \tau & \tau^2 & \tau^3 \\
1 & \tau^2 & \tau^3 & \tau^4
\end{bmatrix}.
$$

In general, the following property is true for the secondary diagonal, which is the diagonal above the main diagonal, in $Z_n$. In $Z_n$, the elements $z_{i-1,i}$, $i = 1, n - 1$ are a sum of elements of the geometrical progression with a ratio $q = \tau^2$ [4]. Thus,

$$
z_{i-1,i} = -\tau^{-i} - \tau^{-i+2} - \tau^{-i+4} - \cdots - \tau^{-i+2(n-1)}.
$$

For simplicity of notation, we define

$$
\tau_i = \sum_{k=0}^{i-1} \tau^{-i+2k} = \sum_{k=0}^{i-1} \tau^{-2k}, \quad i = 1, n - 1.
$$

Therefore,

$$
z_{i-1,i} = \tau_i.
$$

**Example 1:** Illustration of the theory discussed is shown for $n = 5$.

$$
Z_5 = \begin{bmatrix}
1 - \tau_1 & 0 & 0 & 0 \\
1 - \tau_2 & \tau_1 & 0 & 0 \\
1 & \tau & \tau^2 & \tau^3 \\
1 & \tau^2 & \tau^3 & \tau^4
\end{bmatrix}.
$$

The matrix $Z_n$ defines an orthogonal transform. We denote this transform as the Golden Fibonacci transform, since it corresponds to the canonical golden Fibonacci sequence [5].
3. PROPOSED ALGORITHM

In this section, we have presented a new Golden-Ration Haar wavelet transforms with image steganography applications.

The integer sequence 0, 1, 2, 3, 5, 8, 13, 21, 34, 55 is called the Fibonacci sequence. It has been the focus of the mathematicians for centuries, and been utilized in various applications in the digital image/signal processing [6]. Fibonacci numbers can be presented recursively as the following:

\[ F_n = F_{n-1} + F_{n-2}, \]

where \( F_0 = 0, F_1 = 1, \) and \( n = 2, 3, \ldots \)

The important property of Fibonacci sequence is that the ratio of any number to its previous number will eventually lead to a limit known as the Golden Mean (1.61804). On the other hand, it should also be observed that the number that following the given number in the sequence has the following equalities:

\[ F_n/F_{n-1} \rightarrow (1.61804). \]

In order to obtain a matrix inverse to the matrix \( Z_n \), is necessary to normalize their columns. In that order, each element in \( Z \) is divided by the sum of squares of elements in the row where the element appears [6].

Based on the Golden Ratio (GR), we will illustrate the construction of the GR-Haar matrices, which ultimately lead to the construction of the discrete GR-Haar wavelet transform.

3.1.1. Construction of GR-Haar Matrices

A square orthonormal matrix with elements \( \alpha f_1 + f_2 \) is called Golden Ratio Haar Matrix, or GR-Haar matrix, where \( \alpha \) is the golden mean, and \( f_1 \) and \( f_2 \) are Fibonacci numbers. It can be shown that the following matrices are symmetric orthonormal GR-Haar matrices of order 2.

\[ \Phi_2(k) = \frac{1}{\sqrt{L_{2k+1}}} \begin{bmatrix} \alpha & \alpha^{-2} \\ \alpha^{-1} & \alpha^{-1} \end{bmatrix} \]

where \( \alpha \) is golden mean, \( L_1, F_1 \), are Lucas and Fibonacci numbers, and \( L_k = L_{k-1} + L_{k-2}, L_0 = 2, L_1 = 1, k \geq 2 \). Furthermore, the first ten Lucas numbers are: 2, 1, 3, 4, 7, 11, 18, 29, 47, 76. Based on these, we can simply generate the Golden-Ratio Haar transform (GRHT) matrices in the following:

\[ GRH_N = \left[ \frac{1}{\sqrt{L_{2k+1}}} \Phi_2 (k) \otimes \begin{bmatrix} \alpha^k & \alpha^{-k} \\ \alpha^{-1} & \alpha^{-1} \end{bmatrix} \right] \]

where \( I_m \) is an identity matrix of order \( m \), \( I_1 = (1) \), \( N = 2^n, n=2,3,4,... \)

In the following example, we have shown the eight point GR-Haar transform matrix construction for the illustrative purposes.

**Example 1:** The eight-point Golden-Ratio Haar Transform matrix can be developed by the following factorization with different values of \( k \):

\[ GRH_8 = G_1 G_2 G_3, \]

where \( G_i \) is the normalized sparse matrices, when \( k = i \), is defined as:

\[
G_1 = \begin{bmatrix}
1.618 & 0.618 & 0 & 0 & \cdots & 0 \\
0.618 & 1.618 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0.5774 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0.5774 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0.5774
\end{bmatrix}
\]
It should be noted that the GR-Haar transform representation is developed for 1-D signals. However, it can be applied to 2-D signals by using the following property:

\[ T_{\text{Block}} = [ GRH ][ \text{Block} ][ GRH ]^T \]  \hspace{1cm} (19)

Eq. (10) simply describes the transformation of the rows and the columns of the given block within the 2-D signals. By continuing this process on the entire signal will provide us the transform via 1-D GR-Haar transform representation.

The 16-point basis function illustrations have been shown in figure 3 (a,b). We have manipulated the \( k \) values of the proposed transform matrices, from which we have observed the differences with the most commonly used Haar transform, and the proposed GR-Haar transform.

Since the trace of the auto-covariance matrix in the transform domain for any unitary transform is invariant, one can judge the performance of a discrete transform by its variance distribution for a random sequence governed by some specific probability distribution [16]. The autocovariance matrix in the transform domain is

\[
G_2 = \begin{bmatrix}
1.618 & 0.618 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1.618 & 0.618 & 0 & \cdots & 0 \\
0.618 - 1.618 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & \cdots & 1 \\
\end{bmatrix}
\]

\[
G_3 = \begin{bmatrix}
1.618 & 0.618 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1.618 & 0.618 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1.618 & 0.618 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1.618 & 0.618 \\
0.618 - 1.618 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}
\]

where \([\Phi(n)]\) is any \((2^n \times 2^n)\) orthogonal transform matrix. The diagonal elements of \( A_n \) are the variances of the transform coefficients \( X_0, X_1, \ldots, X_{N-1} \), where \( N = 2^n \). Figure 4 has shown the performance comparison of the three discrete orthogonal transforms, such as Walsh-Hadamard, Haar, and the proposed GR-Haar transforms [16]. It is therefore desirable to have a few transform coefficients with large variances (consequently the remaining transform coefficients will have small variances).
Figure 4: The variance distribution for discrete Walsh-Hadamard, Haar, and GR-Haar transform for $N = 32$

It should also be observed that the variances represent the energy or information content of the corresponding transform coefficients, therefore the transform coefficients with large variances are candidates containing significant features which can be utilized in pattern recognition application [17].

Figure 6: Proposed GR-Haar Wavelet transform decomposition on the test image (a), in (a) $k = 2$, (b) $k = 8$.

Figure 7: Commonly used Haar Wavelet Transform on color image.

Figure 8: Proposed GR-Haar Wavelet transform decomposition on the test image, (a) $k = 2$, (b) $k = 4$.

4. EXPERIMENTAL RESULTS

This section briefly discusses the results that obtained from the experimental analysis. In this analysis several cover images (size 512x512) were embedded using 2 Kb and 6Kb of secure data. Table 1 and 2 illustrate the amount of error (RMSE) introduced by the presented technique while using different golden ratio powers ($k$). Note that when the power ($k$) is equal to zero the transformation is equivalent to the Haar wavelet. It can be observed that the presented method introduces less error after embedding when $k = 8$.

Table 1: Error (RMSE) comparison of embedded (2Kb) images with different golden ratio powers ($k$)

<table>
<thead>
<tr>
<th>k</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>5_pedal</td>
<td>0.234</td>
<td>1.029</td>
<td>0.448</td>
<td>0.261</td>
<td>0.108</td>
</tr>
<tr>
<td>Golden Gate</td>
<td>0.236</td>
<td>1.271</td>
<td>0.524</td>
<td>0.257</td>
<td>0.086</td>
</tr>
<tr>
<td>flag</td>
<td>0.234</td>
<td>1.121</td>
<td>0.467</td>
<td>0.260</td>
<td>0.103</td>
</tr>
<tr>
<td>barn</td>
<td>0.232</td>
<td>0.924</td>
<td>0.446</td>
<td>0.262</td>
<td>0.113</td>
</tr>
<tr>
<td>Trolley</td>
<td>0.235</td>
<td>1.131</td>
<td>0.485</td>
<td>0.259</td>
<td>0.096</td>
</tr>
<tr>
<td>Chess Match</td>
<td>0.230</td>
<td>1.031</td>
<td>0.453</td>
<td>0.260</td>
<td>0.112</td>
</tr>
<tr>
<td>bee</td>
<td>0.234</td>
<td>1.006</td>
<td>0.451</td>
<td>0.261</td>
<td>0.108</td>
</tr>
</tbody>
</table>

Table 2: Error (RMSE) comparison of embedded (6Kb) images with different golden ratio powers ($k$)

<table>
<thead>
<tr>
<th>k</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>5_pedal</td>
<td>0.353</td>
<td>1.802</td>
<td>0.799</td>
<td>0.426</td>
<td>0.219</td>
</tr>
<tr>
<td>Golden Gate</td>
<td>0.378</td>
<td>2.028</td>
<td>0.911</td>
<td>0.453</td>
<td>0.200</td>
</tr>
<tr>
<td>flag</td>
<td>0.357</td>
<td>1.865</td>
<td>0.820</td>
<td>0.426</td>
<td>0.217</td>
</tr>
<tr>
<td>barn</td>
<td>0.350</td>
<td>1.570</td>
<td>0.778</td>
<td>0.425</td>
<td>0.226</td>
</tr>
<tr>
<td>Trolley</td>
<td>0.366</td>
<td>1.937</td>
<td>0.862</td>
<td>0.435</td>
<td>0.211</td>
</tr>
<tr>
<td>Chess Match</td>
<td>0.355</td>
<td>1.755</td>
<td>0.804</td>
<td>0.429</td>
<td>0.218</td>
</tr>
<tr>
<td>bee</td>
<td>0.357</td>
<td>1.849</td>
<td>0.817</td>
<td>0.424</td>
<td>0.216</td>
</tr>
</tbody>
</table>
Experimental results have shown that embedding in the GR-Haar Wavelet transform decomposition can provide different parametric values (k). The parameter (k) in this case can in fact reduce the amount of error introduced to the image after embedding. In our results k=8 has shown the best results. The presented method has also produced better results than the commonly used Haar Wavelet Transform.

5. CONCLUSION

In this paper, we have presented a parametric golden ratio-Haar wavelet, and the application for the multimedia data hiding. We have shown the proposed transform’s properties with illustrative examples. Furthermore, the analysis on the data hiding technique has given better results when compared to the commonly used Haar wavelet based steganographic approaches.

6. ACKNOWLEDGMENTS

This research was partially funded by the Center for Infrastructure Assurance and Security at University of Texas San Antonio.

7. REFERENCES