

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim\*

Department of Computer Science – University of Technology – Iraq

\*[110104@uotechnology.edu.iq](mailto:110104@uotechnology.edu.iq)

Received: 10 October 2018

Accepted: 13 January 2019

### Abstract

Nowadays, due to the accelerated advancement of internet and multimedia technology, transmission and spreading of multimedia data have become very easy work. This has become a thoughtful threat to the owners of multimedia content. Therefore, a major attention has been given to multimedia data copyright security. In this paper, the proposal of an audio watermarking algorithm that is secure, robust, and blind for copyright security was presented. Decomposing the audio signal is made first with Discrete Wavelet Transform (DWT), thereafter selecting the coefficient of low-frequency which then made into frames. Next, on each frame, Discrete Cosine Transform (DCT) is directed. The essential features are concluded from the entered audio signal, then these features are encoded to produce Quick Response (QR) code to produce the watermark image, and by a novel technique which utilizes Rubik's cube, this watermark image is next encrypted. Later the watermark bits are implemented into DCT coefficient by Quantization Index Modulation (QIM) determined by frame number. The results of experiments imply that this algorithm is strong against numerous signal strikes, unnoticeable and has an elevated average Signal to Noise Ratio (SNR) value reaches 61 dB.

**Keywords:** Audio watermarking, Rubik's cube, QR code, DWT, DCT.

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

## استخدام مكعب روبيك في تشفير العلامة المائية الصوتية الهشة

رنا محمد حسن و مثيل عمادالدين عبدالمنعم

قسم علوم الحاسوب – الجامعة التكنولوجية

الخلاصة

في الوقت الحاضر، بسبب التطور المتسارع في تكنولوجيا الإنترنت والوسائط المتعددة، أصبح نقل ونشر بيانات الوسائط المتعددة عملاً سهلاً للغاية. الذي أصبح تهديداً مدروساً لأصحاب محتويات الوسائط المتعددة. لذلك، تم إيلاء اهتمام كبير لأمن حقوق النشر لبيانات الوسائط المتعددة. في هذا البحث، تم تقديم اقتراح الخوارزمية الصوتية بالعلامة المائية التي هي آمنة وقوية وعمياء لأمن حقوق التأليف والنشر. يتم إجراء تحليل الإشارة الصوتية أولاً بتحويل الموجات المنفصلة (DWT)، بعد ذلك اختيار معامل التردد المنخفض الذي بعد ذلك يحول الى اطر في كل إطار يتم توجيه تحويل (DCT). يتم الحصول على الميزات الأساسية من كل إشارة صوتية، وبعد ذلك سيتم ترميزها لإنتاج رمز الاستجابة السريعة كصورة مائية مكيفة، وبتقنية مقترحة تستخدم مكعب روبيك هذه الصورة بالعلامة المائية المشفرة. في وقت لاحق يتم زرع بتات العلامة المائية في معامل DCT عن طريق تعديل مؤشر التكمية QIM يتم تحديده بواسطة رقم الإطار. تشير نتائج التجارب إلى أن هذه الخوارزمية قوية ضد العديد من المؤشرات الرقمية، والتي كانت غير ملحوظة ولها قيمة مرتفعة للإشارة إلى نسبة الضوضاء (SNR) يصل إلى 61 dB.

**الكلمات المفتاحية:** العلامة المائية الصوتية، مكعب روبيك، ترميز QR ، النقل الموجي، النقل كوساين.

Introduction

Media can be distributed by the author using web pages or any other communal methods. Therefore, any person is able to copy the author's media. Thus, copiers may claim that they own these media. This problem can be solved by using extra information that is entrenched into media like information of license, author or copyright security. Digital watermarks are either observable or unobservable from the individual eyesight [1].

The one that is more invasive to the media are the observable watermarks. Such as the station's logo in the corner of the screen which can be viewed clearly on the majority of network

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

television stations is an example of such watermarks. Therefore, the removal of this watermark will be the obvious goal of the attackers [2].

Three parameters are considered during the planning of a watermarking algorithm: robustness, capacity and imperceptibility. The watermark capability to stay legible following inadvertent or cruel processing on the signal is referred to as robustness, whereas the sum of bits which are able to be entrenched into a multimedia is referred to as capacity. Lastly, the decomposition presented into the signal is referred to as imperceptibility. These three parameters are contradicted to one another, and the choosing of these parameters depends on the necessities of the application [3].

An enormous attention has been given to the digital audio watermarking as they afford effective solutions for the protection of digital media [4]. It is the procedure of embedding or concealing a watermark in the form of audio, image, or text into an original audio signal. Afterward, the embedded data may be obtained or detected from the marked signal for the purpose of numerous applications like content verification, finger printing, broadcast monitoring and copyright protection [5].

One of the newest focuses of research lately is the content verification, methodologies are required in the various real application so as to guarantee that when transferring something to somewhere, it is delivered as is. The suitable methodology must be naive and protected to guarantee the validity of the work [6]. Watermarking an image or video is somewhat simpler comparing to watermarking an audio signal, due to the sensitivity of Human Auditory System (HAS) over the Human Visual System (HVS). [5].

Digital watermarking of audio is additionally classified into robust watermark, semi-fragile watermark and fragile watermark depending on the precise reason. A fragile watermark can be affected by every minor change of the original multimedia file therefore, can be utilized to confirm its integrity. A semi-fragile watermark is capable of resisting certain popular signal operations nonetheless it is sensitive to malicious tampering. A robust watermark is utilized to copyright protection because it can resistant different signal attacks [6].

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

The chief requests of watermarking the digital audio are Robustness, data capacity, and imperceptibility. More specifically, the watermark must be inaudible within audio data of the host, in order to preserve the quality of the audio. Lastly, the extraction of the watermark to verify ownership should be straightforward [4]. Various watermarking methods of different complexities have been proposed, in [7] the bits of the watermarking are embedded into the frames peaks on which Discrete Fourier Transform (DFT) has been executed. The Fourier transformation usage is restricted only to linear systems and stationary data series. In [8] the host audio signal is decomposed by the use of Discrete Wavelet Transform (DWT) into various multi-resolution sub-bands.

The sub-band with the highest resolution is chosen to embed the watermarking bits. This scheme manifests to be promising to take into account the limitation of the Fourier transform, however still shows a limitation that the fundamental functions of wavelet transformation are static and do not necessarily match the shape of the considered data series in each instant in time [9].

Lately, a novel signal decomposition technique mentioned as Empirical Mode Decomposition (EMD) has been presented in order to overcome this issue by analyzing non-stationary and nonlinear signals in a totally adaptive way, as presented in our former work [10].

This paper proposes an efficient fragile audio watermarking that fulfills the requirement of inaudibility and security, depending on EMD for audio content authentication and encrypt it using a new strategy encryption using Rubik's cube.

The rest of this paper is organized as follows; in section 2 EMD theory is reviewed. Section 3 review the Rubik's cube fundamentals, the QR code described in section 4 that presents the synchronization code. Section 5 presents the proposed watermarking embedding and extracting algorithms and the performance analysis and experimental results are shown in Sections 6 and 7 respectively. Finally, the concluding remarks are presented in the final section.

## Empirical Mode Decomposition (EMD) Fundamental

The decomposition of an audio signal into a set of Intrinsic Mode Functions (IMFs) and a final residual is done by using EMD. The IMF was explained by Huang and it must fulfill the next two situations concurrently [11]:

Within the whole set of data, the zero-crossing number and extrema must be equalized or not equalized at maximum by 1.

In every case, the envelope mean value express by (local maxima or minima) is equal to 0.

A chief benefit of EMD depends on a priori selection of basic functions or filters. As comparing it with the approaches based on the classical kernel, EMD is a totally data-driven technique which recursively decomposes whichever signal into a number of zero mean components named IMFs.

Assume the mentioned signal  $x(t)$  can be decomposed from finer scales to coarser ones as the sum of  $n$  number of IMFs and a final residual as follows, as one can see in figure (1) [11].

The IMFs are almost orthogonal to one another and altogether have approximately zero means. The number of extrema will decrease as moving from a particular mode to the following, the entire decomposition is assured to be finished with a finite number of modes. The IMFs are totally defined by their local extrema and therefore they are recovered utilizing their extrema [11].

Greater order IMFs such as low-frequency mode considered signal dominated, thus signal degeneration can be the result of their modification. As consequence, the finest locations for the robust placement of watermark are these modes [11]. However, the entrenchment of watermarks into the mode of great frequency for example lower order IMFs considered chiefly sensitive to attacks. Thus, as proposed in this paper, the finest location for the fragile watermark placement appears to be these modes.

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

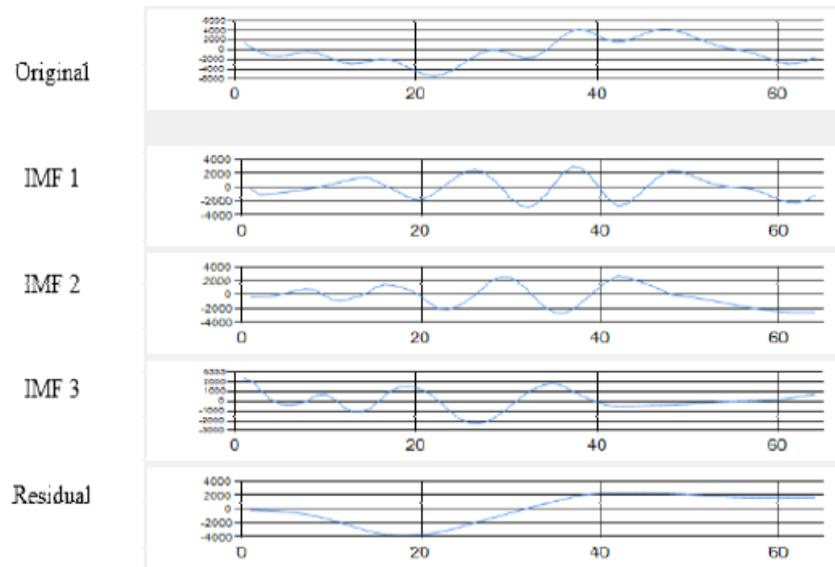


Figure 1: Decomposition of an audio signal with EMD

### Rubik's Cube

Rubik's cube is a type of plaything, that is divided into various subcubes. In  $n \times n \times n$  Rubik's cube, one sub square is covered by one sticker, hence each of the six square are covered by  $n \times n$  stickers. Each column can be rotated clockwise or anticlockwise around one axis. As the columns being rotated, a specific picture can be pieced together on the surface of the Rubik's cube as seen in figure (2) [12].



Figure 2: Rubik's cube

Using Rubik’s Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

Three different ways can the Rubik’s cube algorithm be performed in combination with the encipher system for data hiding as shown in Figure (3).

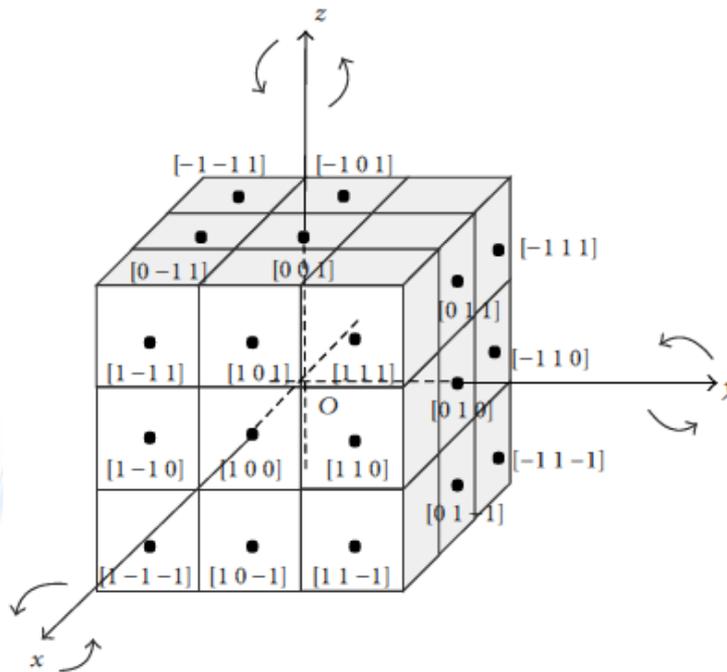


Figure 3: Rubik's cube directions

When the hidden data undergo encryption via an encipher system, the detail process is addressed. Afterward, by implementing Rubik’s cube algorithm the encrypted data is scrambled. Lastly, the scrambled data is next entrenched into a cover/host image to attain data concealing and obtain a stego-image as demonstrated in figure (4) [13].

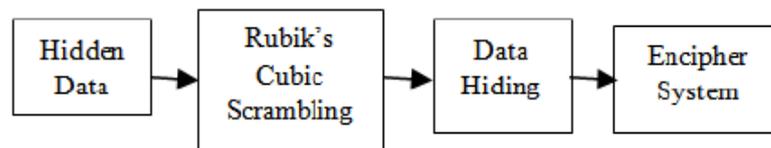


Figure 4: Data concealing based on the combination of enciphers system and Rubik’s cube

Rubik’s cube owns 6 faces and may be partitioned into 54 parts (six faces\*3\*3). At first, the concealed data which are treated such as an image are divided into various unit block size like pixel based, 3\*3 pixels based, or another n\*n pixels based. Afterward, 54 units are chosen

Using Rubik’s Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

consecutively then converted into six faces depending on the 6 faces of the Rubik's cube by designing an index number as illustrated in Figure (5).

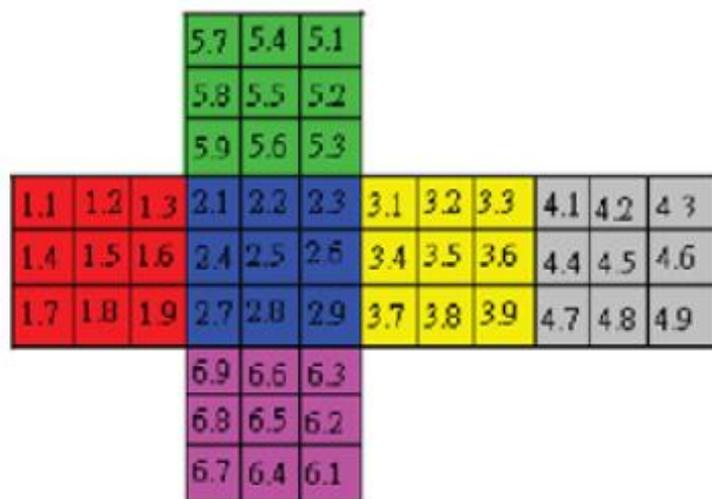


Figure 5: Corresponding Index of a Rubik’s Cube

Thus, the signal may be divided into plenty of various 54 blocks units and created plenty of various Rubik's cube. To utilize the Rubik’s cube for data concealing, the basic process unit may be a single pixel, small block, or macrocell (large block) as compared to the classical Rubik’s Cube. To put back the Rubik’s Cube into the original style, one can follow the reverse step of rotation or following the decomposition steps of restoring the Rubik’s cube. As the application of Rubik’s cube can scramble the sequence of an original sequence, it can be used for data encryption or data hiding.

During the processing, a person can simply discover that the cube positioned in the center, sides and corner are moved just to the center, sides and corner positions respectively. Nonetheless, the corner cube owns three faces [12].

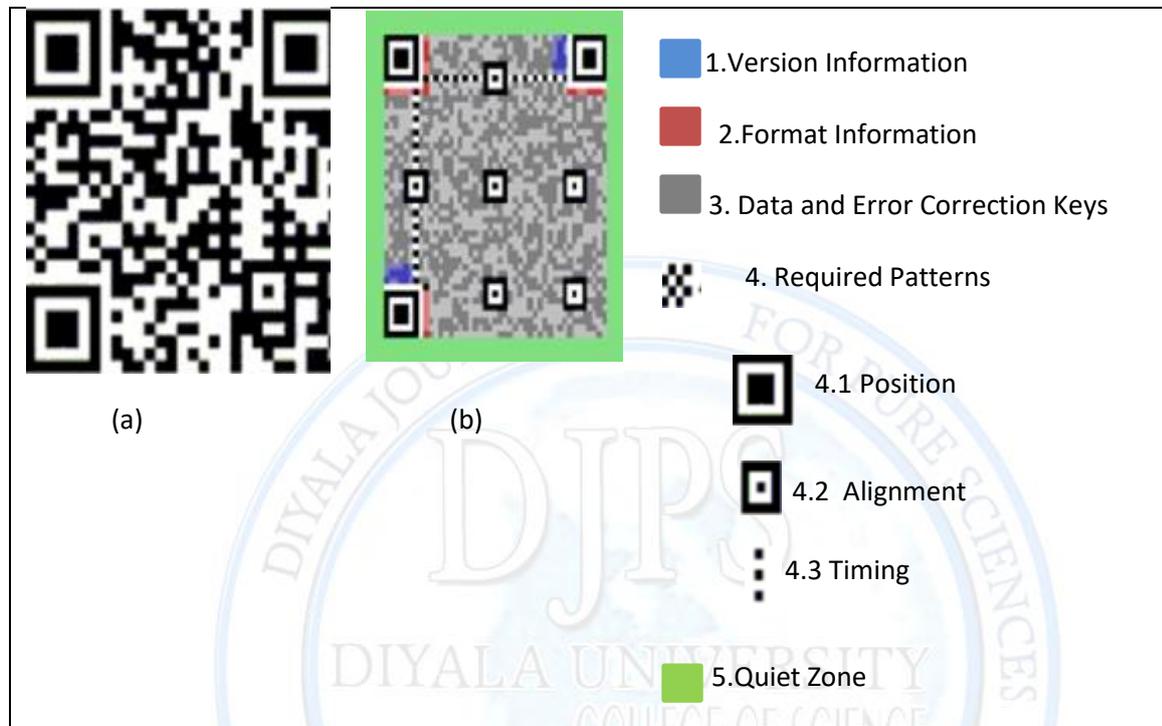
**The Quick Response (QR) Code**

As comparing the 1D bar code to the 2D QR Code that is in the form of matrix code, the QR Code has greater density, the bigger capacity of storage, more robust performance of error correction and safety. This QR code was created in 1994 by Denso Wave [14]. It has the ability to store huge alphanumeric information and simply readable via scanner. A QR code is able to

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

be read in 360 degrees from every direction therefore, removing interference [15]. A person can view the QR image in figure (6).



**Figure 6:** QR code; (a) A QR Code Image. (b) Structure of the QR Code

### Proposed Audio Watermarking Technique

The methods of time domain watermarking considered helpless towards hackers attacks such as compressing, resampling and low pass filtering. Which implies that watermarks which are hidden can be simply ruined. Otherwise, methods of frequency domain watermarking are stronger towards hackers attacks, therefore they are considered superior for copyright security as demonstrated within this paper. Recently, the introduction of the transforms technique to digital watermarking of audio has been made. DWT is a type of these transforms, that is vastly common in the applications of digital signal processing. During audio watermarking that utilizes DWT, the audio signal is first decomposed into many frequency sub-bands. Next, the embedding of the watermark bits into the coefficients of one or more sub-bands is done by utilizing the Quantization Index Modulation (QIM).

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

DWT is quicker as compared to the other transforms and in addition, it is reasonably strong against compressing attacks [11]. Another transform which has been utilized in the applications of audio watermarking is the DCT. By employing the QIM, the DCT entrenches the digital watermark into the acquired coefficients from the transform. The bits of the watermark is embedded in the sections of great energy in the host audio signal which results in a vastly pure watermarked sound, therefore this approach has a great SNR.

Furthermore, DCT is susceptible to compressing attacks, while it is strong against low pass filtering and resampling attacks. Therefore, it is possible to join two or more of the watermarking methods in order to enhance the functioning and the robustness of the audio watermarking technology. Moreover, the watermark data can be encrypted by utilizing encryption technique.

The Rubik's cube is an old toy which can be employed as an encryption technique. This paper gives a method that uses both DCT and DWT for watermarking of audio by utilizing QIM for copyright security, also encrypt watermark image by utilizing Rubik's cube. Figure (7) gives the proposed system block diagram. This combined technique demonstrates great SNR and robust against different attacks.

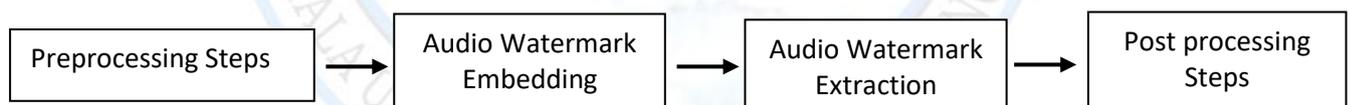


Figure 7: The Proposed System Block Diagram

### 1. Preprocessing

There are few preprocessing steps that precede the embedding and the extraction process of the watermark algorithm construction. These preprocessing steps are demonstrated in figure (8):

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

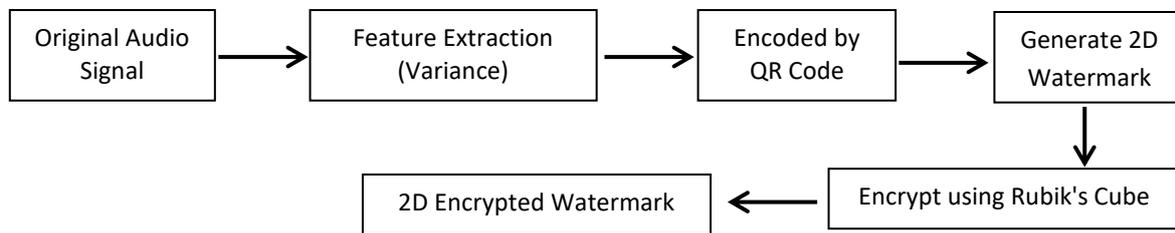


Figure 8: Preprocessing Steps

**A. Audio Feature Extracting**

Instead of entrenching the data of the watermark within the audio signal of the host like the traditional watermarking algorithms, in this paper the fundamental features are extracted from the audio signal of the host, next the utilization of these features for the recovery of the watermark. The audio signal has a lot of features which can be extracted from. Within this paper, the signal power density (variance) measurement can be chosen as a selected feature.

**B. QR Code Image Generation**

Regarding benefits of QR code, in order to produce the 2D QR code image, the variance value of the audio signal is encoded with the encoding algorithm of QR.

**C. Watermark Image Encryption**

The extraction of the entrenched watermark can be done if the procedure of entrenching is known. Nevertheless, the watermark encryption process must precede the entrenching process in order that the elimination of the watermark by the attackers becomes impossible. Among the various encryption algorithms which are used for the encryption of image, the one that considered proper for practical use are the encryption techniques depended on the Rubik's cube. Since they give a good combination of complexity, high security, computational power and speed. Thus, in this paper, the encryption of the QR code image which is acquired from the former step is made by using Rubik's cube in order to enhance the security. However, the QR code images are permanently squares. The encryption process is demonstrated in figure (9).

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

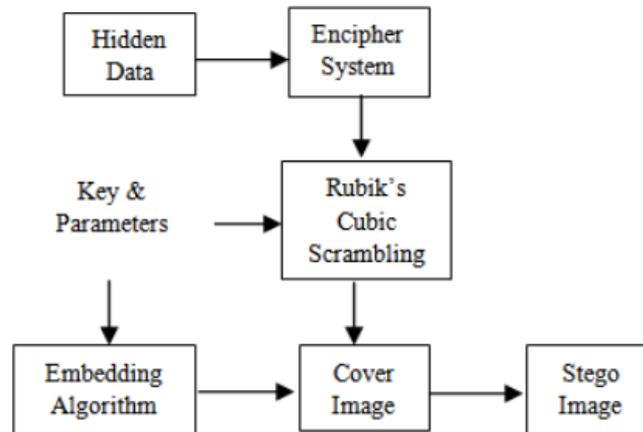


Figure 9: Encryption process

## 2. Audio Watermarking Algorithms

This proposal is depended on the frequency domain approach based on hybrid transformation. By utilizing QIM, the embedding and extracting process is made. To guarantee security, the watermark image is encrypted initially. One benefit of employing hybrid transformation in the frequency domain is to guarantee a great degree of robustness during hackers attempts. Therefore, the idea of this proposal is to conceal an encrypted watermark image in the frequency domain within the original audio signal. Primarily, by utilizing DWT the input audio signal is decomposed into an appropriate wavelet basis. Next, the selection of the low-frequency coefficient of the decomposed signal is made, afterward using DCT on every frame acquired from WT. By using QIM the bits of the watermark are entrenched in either the first ac-component or the dc-component of every frame acquired from DCT according to whether the frame is odd numbered or even respectively. In another meaning, the embedding position will be dc-component if the frame number is even, while the embedding position will be first ac-component if the frame number is odd. As seen, the frames number should be appropriate with the sequence length of the watermark where one can insert just two bits in every frame.

Firstly, Rubik's cube is utilized for encryption by scrambling the bits sequence within the image applying Table 1 which utilized to transmit the positions according to the degree of rotations. Algorithm 1 demonstrate the steps for encrypting algorithm.

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

**Algorithm 1:** Image Encryption using Rubik's Cube**Input:** Two-dimension QR code Watermarked Image W**Output:** Two-dimension QR code Encrypted Watermark Image W'.**Begin:****Step 1:** Set the pre-define initial values  $X_1$ ,  $Y_1$  and  $Z_1$ .**Step 2:** By using Rubik's cube, generate the Rubik's sequence X, Y, and Z with  $N*N$  length.**Step 3:** Generate the binary sequence B from the Rubik's sequences X, Y, Z with same Length by using threshold value division method as follow:
$$\text{If } X_k < \text{threshold, then: } B_k = 0$$

$$\text{Else if } X_k \geq \text{threshold, then: } B_k = 1$$
**Step 4:** Convert the values of B to  $X_2$ . And so on to generate  $Y_2$  and  $Z_2$ .**Step 5:** Select the digit from (3 to -3) randomly to choose the rotation operations.**Step 6:** The XOR operation is performed between the watermark image W and the sequences to conclude the sequence E that is encrypted:

$$E = \{ e_0, e_1, e_2, \dots, \dots, \dots, e_{N-N} \}$$

**Step 5:** Finally, the encrypted sequence E is converted to two-dimension watermark image W'.**End.**

Following the accomplishment of the entrenching process, is the application of IDCT on the coefficients that have been modified for every frame, then the frames will be concatenated.

The application of IDWT is made by taking the adjusted coefficients with low frequency and the unchanged residual components. Lastly, the watermarked audio signal is the resulted signal.

During the extraction process as in the entrenching process, by utilizing DWT the watermarked audio signal is decomposed initially. Next, the selection of the coefficient with a low frequency of the decomposed signal is made. The chosen coefficient will be divided into frames and afterward, on every frame, the DCT is applied. Subsequently, by utilizing QIM the data of the watermark are extracted.

Using Rubik’s Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

The original signal is not required for the extraction of the watermark as the proposed technique is blind. The algorithms of entrenching and extracting are explained as follows:

**A. Watermark Embedding**

Subsequent to the preprocessing step, a two-dimension encrypted QR code is acquired as a watermark image symbolizes by  $W'$ . Next, the two-dimension image is transformed to a one-dimension sequence of bits for embedding, symbolized by  $N(i) \in \{0, 1\}$ . The entrenching of the binary sequence will be either into first ac-component or dc-component of every acquired frame from DCT according to the number of the frame via employing QIM which is demonstrated in the equations below:

**Table 1:** Rubik's Cube Rotations

Parameters	Operations	
	Digit	Rotation
X1, x1, Y1, y1, Z1, z1	3	Clockwise rotating 270 <sup>0</sup> along X-axis, Y-axis, or Z-axis according to the digits
	2	Clockwise rotating 180 <sup>0</sup> along X-axis, Y-axis, or Z-axis according to the digits
	1	Clockwise rotating 90 <sup>0</sup> along X-axis, Y-axis, or Z-axis according to the digits
	0	No rotation or shift performed
	-1	Counter- Clockwise rotating 900 <sup>0</sup> along X-axis, Y-axis, or Z-axis according to the digits
	-2	Counter- Clockwise rotating 180 <sup>0</sup> along X-axis, Y-axis, or Z-axis according to the digits
	-3	Counter- Clockwise rotating 270 <sup>0</sup> along X-axis, Y-axis, or Z-axis according to the digits

$$A^4(dc) = [A (dc) /g^2 ] * g^2 + (3 * \frac{g^2}{4}) \tag{1}$$

$$A^4(dc) = [A (dc) /g^2 ] * g^2 + (\frac{g^2}{4}) \tag{2}$$

$$A^4(ac) = [A (dc) /g^2 ] * g^2 + (3 * \frac{g^2}{4}) \tag{3}$$

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

$$A^4(\text{dc}) = \lceil A(\text{dc}) / g^2 \rceil * g^2 + \left( \frac{g^2}{4} \right) \quad (4)$$

The audio signal of the host is symbolized by A whereas A' refers to the watermarked signal, dc and ac symbolize to the position of entrenching in DCT coefficient while the entrenching strength selected to preserve the inaudibility constraint is symbolized by g, the floor function is symbolized by  $\lceil \rceil$ . The steps of the entrenching process are illustrated in figure (10), then the algorithm of watermark entrenching is subsequently shown in the algorithm 2.

**Algorithm 2:** Embedding the watermark

**Input:** The audio signal (A) that is original, Encrypted watermark bit sequence N

**Output:** The audio Signal A' that is watermarked.

**Begin:**

**Step1:** Using DWT to decomposed input audio signal A.

**Step2:** From the decomposed signal, choose the low-frequency coefficient.

**Step3:** Separate the low-frequency coefficient into two equal frames.

**Step4:** On each frame, apply DCT.

**Step5:** Using QIM, embed the watermark sequence into the coefficient of DCT:

If frame number is even then

Begin

For i=1 to Number of frames

If F(i) equal to 1 then execute equation (1)

Else if F(i) equal to 0 then execute equation (2)

End

Else if frame no. is odd then

Begin

For i=1 to Number of frames

If F(i) equal to 1 then execute equation (3)

Else if F(i) equal to 0 then execute equation (4)

End

## Using Rubik's Cube in Fragile Audio Watermark Encryption

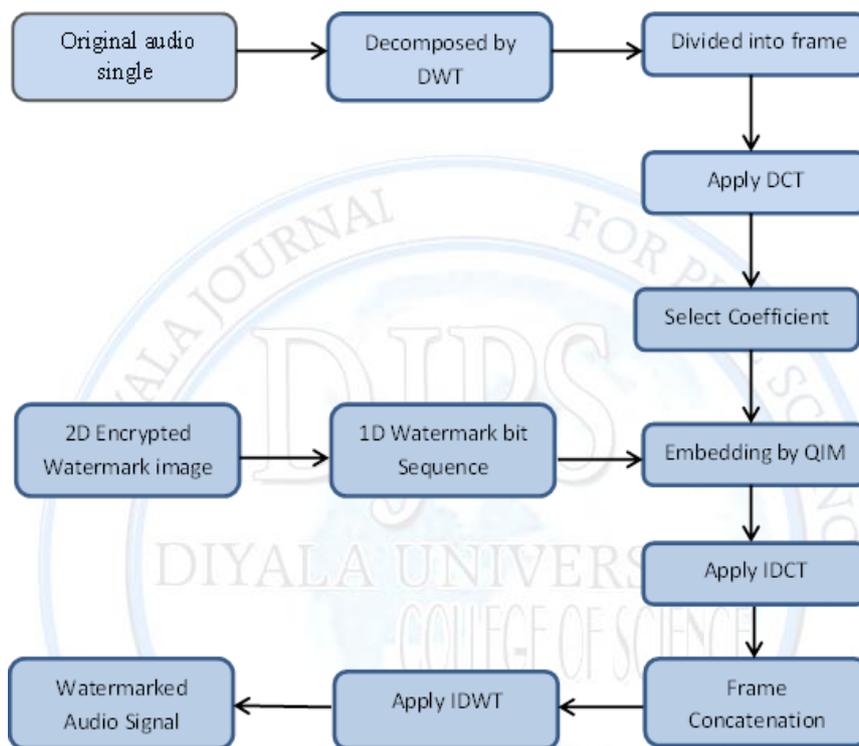
Rana M. Hassan and Matheel E. Abdulmuim

**Step6:** On each converted frame, apply inverse DCT.

**Step7:** add frames to reconstruct the low-frequency coefficient of DWT.

**Step8:** Apply inverse DWT to obtain the watermarked audio signal A'.

**End.**



**Figure 10:** Watermark Embedding Process

## B. Watermark Extraction

During the process of extraction, the decomposition of the audio signal that has been watermarked is made firstly. Next, the coefficient with a low frequency of the decomposed signal is picked. Afterward, the chosen coefficients will be divided into equivalent frames. On each frame the DCT is applied and subsequently, by applying QIM, the extraction of the data bits of the watermark from DCT coefficient is made precisely from either first ac component or dc-component depending on the number of the frame. The process of extraction doesn't utilize the original audio signal. Figure 11 demonstrates the steps of the extracting process, and the algorithm of watermark extraction is shown subsequently in the algorithm 4.

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

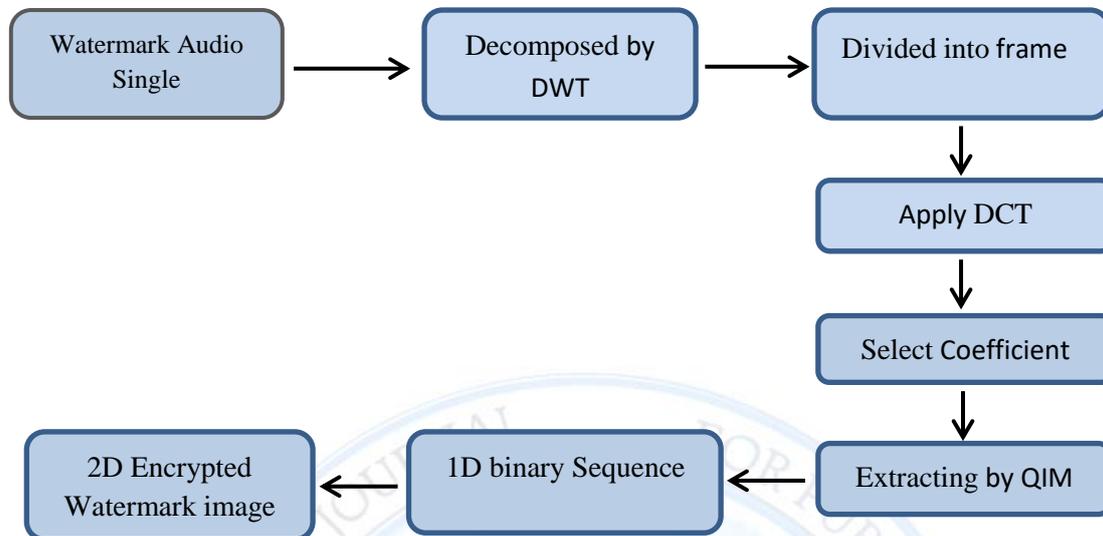


Figure 11: Watermark Extraction Process

**3. Post Processing**

Following the 2D encrypted watermark image extraction, there are some post-processing steps which are summarized as follows:

- 1. Watermark Image Decryption:** Within encryption process, the decryption of the extracted 2D watermark image is done by utilizing the Rubik's cube which produces a random sequence to decrypt the image.
- 2. QR Code Image Decoding:** By using the decoding algorithm of the QR code, the obtained 2D QR code image from the process of decryption undergo decoding to obtain the variance value of the audio signal that has been watermarked.
- 3. Feature Extracting:** From the watermark audio signal fundamental features are extracted, mainly a signal power density measure (Variance). So as to guarantee the copyright protection, the features variance value extracted from the watermark audio signal and the variance value gained from decoding the QR code watermark image should be identical.

**Performance Analysis**

The proposed algorithm performance in terms of data payload, Signal to Noise ratio (SNR), Bit Error Rate (BER), Mean Opinion Score (MOS) and Normalized Correlation (NC) is evaluated.

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

Depending on the recommendations of International Federation of the Photographic Industry (IFPI), the watermark audio signal must preserve greater than 20 dB SNR [1].

Five participants were chosen to hear the original and watermarked audio signal and were demanded to state the differences between the two. The outcome of this test is an average of the quality ratings named MOS, MOS gauge from insignificant to very bothersome. The BER and the NC were utilized to estimate the accuracy of the watermark image detection. To evaluate watermark detection accuracy after signal processing operation, the BER is used.

NC assess the likeness between the original watermark and the extracted one. When the NC value is low that indicates lack of watermark, whereas great NC value refers to the existence of watermark. The payload can be utilized, that quantifies the sum of data to be concealed. More specifically, the data payload indicates the bits number which is entrenched into the audio signal during a unit of time which is measured in the unit of bits per second (b/s).

### Experimental Results

In order to demonstrates the paper effectiveness, "classic-music, Arabic-music, french-song, and speech" is the mono audio signal that the emulation is made on in wave format sampled at 44.1 kHz with depth set to 16-bit, the duration of each audio signal is (3.12 ,2.44, 1.12, and 2.3) minutes respectively. The level of DWT decomposition is placed to 3, the size of the frame is 32 sample per frame. The watermark data that has been entrenched is adaptive in this proposal. Every audio signal possesses watermark data for its own. Thus, the extraction of the value of the variance feature from each audio signal is done first, afterward for the resulted value a binary QR code image is created as shown in the table 2. Every QR code watermark image has a size of 10000 bits ( $M*N=100*100$ ). To guarantee this proposal security, the encryption of the two-dimension QR code image is made via utilizing Rubik's cube with primary value  $x1 = 0.7$ ,  $y1=0.6$ ,  $z1=0.5$  these selected parameters guarantee a great degree of security. Table 2 demonstrates the encryption watermark image for every audio signal. Next, the conversion of the encrypted two-dimension watermark image into one-dimension sequence to be inserted either into first ac-component or dc-component location of DCT coefficient, a single bit is

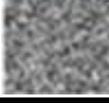
Using Rubik’s Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

inserted in each location. In addition, value of  $g$  is fixed to 5. The parameters were chosen by experiment to attain a good compromise between robustness, payload and imperceptibility.

Table 3 demonstrates the MOS and SNR measuring for every audio signal. Every value of SNR exceeds 20 dB displaying the proper selection of  $g$  value also the corroborative to IFPI standard. In addition, each value of MOS of the audio signals that have been watermarked is 5, that confirms the watermark signal imperceptibility. The watermarks image that has been extracted following decryption with the associated values of BER and NC for every audio signals are demonstrated in the table 3. All values of BER= 0 % and all values of NC= 1. Every QR code images that have been extracted can be successfully decoded. The results prove the watermarking schema effectiveness of various audio signals. In addition, in term of payload, the proposed method has 70 bits per second.

**Table 2:** The generated and encrypted watermarks for the chosen audio signals

Audio Signal	Select Variance Feature	Generate OR code Watermark Image	Encrypted Watermark Image
<i>Arabic-Music</i>	2075		
<i>Classic-Music</i>	4751		
<i>French-Song</i>	6101		
<i>Speech</i>	621		

**Table 3:** The generated and encrypted watermarks for the chosen audio signals

Audio Signal	SNR	MOS
<i>Arabic-Music</i>	56.95	5
<i>Classic-Music</i>	72.36	5
<i>French-Song</i>	53.27	5
<i>Speech</i>	53.38	5
<i>Average</i>	58.99	5

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

**Robustness Test**

So as to assess our robust watermarking scheme work performance, the robustness test is demonstrated within this method to reveal the capability of copyright security. Because the data of the watermark was entrenched in the frequency domain and low-frequency component of audio signal. This gives rise to the capability of robustness of this proposed schema against different kinds of attacks. Thus, to every host audio signal, various forms of attacks such as (re-sampling, filtering, adding noise, re-quantization, cropping and compression) are used. Afterward, for each hacker's attempts, the extraction of the watermark image with the associated values of NC and BER from the manipulated host audio is made.

Table 4 illustrates the robustness test of the watermark signals on Arabic-Music Audio Signal following different attacks. A person can view watermarks that have been extracted together with the related values of NC and BER for various attacks to every audio signal. The decoding can be done successfully for every extracted QR code images which give rise to the capability of this proposal to resist different kinds of attack for various audio signals.

**Table 4:** Robustness test

Attacks Type	BER%	NC	Can be Decoder?	Extracted Image
Re-Quantizing	0	1	Yes	
Resampling 16 KH Z	0	1	Yes	
Filtering	0	0.9998	Yes	
Adding Noise	0	0.9579	Yes	
Cropping	0	1	Yes	
Compression	0	1	Yes	

**Using Rubik's Cube in Fragile Audio Watermark Encryption****Rana M. Hassan and Matheel E. Abdulmuim****Conclusions**

In this paper, a proposal of a robust audio watermarking schema based on hybrid transformation in the frequency domain is made and the watermark is entrenched in great energy DCT coefficient, therefore attaining resistance against different attacks on the signal. The system of watermarking owns a particular degree of capability for error correction since watermark image is QR code, which also improves the effectiveness. Plus, the data of the watermark is adaptive when every signal possesses a watermark image of its own created from the signal feature. Moreover, the watermark image was encrypted to guarantee security and robustness. In addition, this proposed schema attained a greater average SNR value in comparison to other audio watermarking methods as demonstrated in the table 4. Furthermore, this method calculations are simple and don't utilize the original audio signal for extracting and the performed experiments of the entrenching strength  $g$  are maintained constant for the entire files of audio.

Future work suggestions involve the human auditory characteristics and psychoacoustic model in the watermarking scheme for better enhancement of the watermarking method functioning. Lastly, it is considered motivating to research if the proposal supports different sampling rates with the same payload.

**References**

1. N. F. Johnson, An Introduction to Watermark Recovery from Images, In: SANS Intrusion Detection and Response Conference, Feb.1999, San Diego, pp.1-23.
2. S. H. Kumar, International Journal of Computer Application, 10, 1 (2011).
3. B. Furht, D. Kirovski, Multimedia Watermarking Techniques and Applications, 1<sup>st</sup> edition. (Taylor, Auerbach ,2006), pp. 1-464.
4. K. Khaldi, A. Boudraa, IEEE Transactions On Audio, Speech, And Language Processing, 21, 13 (2013).
5. V. Neethu, R. Kalaivani, Efficient and Robust Audio Watermarking for Content Authentication and Copyright Protection, In: International Conference on Circuit, Power and Computing Technologies 2016, United States, pp.144-147.

## Using Rubik's Cube in Fragile Audio Watermark Encryption

Rana M. Hassan and Matheel E. Abdulmuim

6. M. Abdulmunem, A. Badr, International Journal of Advanced Research in Computer Science, 8, 5 (2017).
7. T. Xu, X. Shao, Z. Yang, Multi-watermarking Scheme for Copyright Protection and Content Authentication of Digital Audio, In: Pacific-Rim Conference on Multimedia, 2009, China, pp.5879-5890.
8. J. Wang, New Digital Audio Watermarking Algorithms for Copyright Protection, PhD Thesis, National University of Ireland, Maynooth, Ireland, (2011).
9. K. Kumar, A robust audio watermarking scheme based on singular value decomposition, M.Sc. Thesis, Jadavpur University, Kolkata, India, (2014).
10. R. Abbas, Color Image Denoising using 3D Wavelet Transform, M.Sc. Thesis, University of Technology, Baghdad, Iraq, (2013).
11. H. Nikmehr, S. Hashemy, A New Approach to Audio Watermarking Using Discrete Wavelet and Cosine Transforms, In: 1st International Conference in Communications and Engineering, 2010, Baluchistan, pp.22-24.
12. W.Yao, P. Ye, X. Li, Discrete Dynamics in Nature and Society, 11, 26 (2014).
13. R. Rhine, N. T. Bhuvan, IJCSNS International Journal of Computer Science and Network Security, 15, 20 (2015).
14. I. Orozco, Software and Hardware-In-The-Loop Modeling of an Audio Watermarking Algorithm, M.Sc. Thesis, University of North Texas, Texas, USA, (2010).
15. F. Abd El-Samie, International Journal of Speech Technology, 12, 27 (2009).