Pamukkale Univ Muh Bilim Derg, 28(2), 324-332, 2022

Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

Regulating watermarking semi-authentication of multimedia audio via counting-based secret sharing

Sayıma dayalı gizli paylaşım yoluyla multimedya sesinin filigran yarı kimlik doğrulaması

Adnan GUTUB[1*]

[1]Computer Engineering Department, College of Computer & Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia.
aagutub@uqu.edu.sa

Received/Geliş Tarihi: 20.05.2021 Revision/Düzeltme Tarihi: 18.06.2021 doi: 10.5505/pajes.2021.54837
Accepted/Kabul Tarihi: 28.06.2021 Research Article/Araştırma Makalesi

Abstract

Watermarking is the process of embedding specific data to prove ownership copyright authentication. It is needed whenever media-files are used without proper permission is granted for authentication accuracy. The current watermarking challenge comes from the ownership proof especially as slight tampering occurs on the audio multimedia file which injure the watermarking causing difficulty in its copyright proof. This paper proposes utilizing counting-based secret sharing strategy to allow validation of ownership correctness watermarking even if some of the multimedia audio-file is interfered, as semi-authentication. The research testing run experimentations showed interesting features although this work is still in its early stage. The authentication verification researched secrecy on the audio's media remarked data altered as on LSB 3 models (1-LSB, 2-LSB, 3-LSB) testing hiding capacity capability as well as PSNR security. Its promising investigation revealed complete data dependency consequences showing real attractive contribution opportunities to be remarked.

Keywords: Audio semi-authentication, Counting-based secret sharing, Digital-watermarking, Information security, Multimedia steganography.

Öz

Filigran, sahiplik telif hakkı kimlik doğrulamasını kanıtlamak için belirli verileri gömme işlemidir. Kimlik doğrulama doğruluğu için uygun izin olmadan medya dosyalarını kullanırken gereklidir. Mevcut filigran sorunu, esas olarak sahiplik kanıtından kaynaklanmaktadır, çünkü ses multimedya dosyasında filigrana zarar veren ve telif hakkı kanıtında zorluklara neden olan hafif bir kurcalama meydana gelir. Bu makale, multimedya ses dosyasının bir kısmı kurcalanmış olsa bile, yarı kimlik doğrulama olarak, sahiplik özgünlük damgasının onaylanmasına izin vermek için sayıma dayalı gizli paylaşım stratejisinin kullanılmasını önermektedir. Araştırma testi çalıştırma deneyleri, bu çalışma hala erken aşamalarında olmasına rağmen ilginç özellikler gösterdi. Kimlik doğrulama doğrulaması, LSB 3 modellerinde (1-LSB, 2-LSB, 3-LSB) olduğu gibi, ses ortamındaki gizliliği, veri test edilmiş gizleme kapasitesini ve PSNR güvenliğini araştırdı. Umut vaat eden araştırması, dikkate alınması gereken gerçek çekici katkı fırsatlarını gösteren tam veri bağımlılığı sonuçlarını ortaya çıkardı.

Anahtar kelimeler: Ses yarı kimlik doğrulaması, Saymaya dayalı gizli paylaşım, Dijital filigran, Bilgi Güvenliği, Multimedya steganografisi.

1 Introduction

Watermarking in digital media-files is becoming an essential tool for claiming responsibility regulations as well as correctness and the traditional ownership proofing [1]. In fact, audio Quran recitation authentication is in real essential need for audio watermarking to proof its narration correctness, as too many unauthentic or fake recitations are found available [2]. Watermarking can be used as judging evidence, assisting verification whenever claiming denial of authorization problem is raised, which is an opposite usage to conventional copyright protection of enforcing permission for legal utilization [3]. Most watermarking newly innovative benefits and applications can be classified as enhancements of these two main categorizations, i.e. claiming responsibility and proof of ownership, such as, owner identification, transaction tracking, broadcast monitoring, usage control, authentication and tamper proofing, persistent item identification, and enhancement of legacy systems [4]. Watermarking can be further classified based on its appearance within the media-files in visible and invisible types applying some steganography data hiding strategies showing clear technical similarities. In fact, the main difference between watermarking and steganography is in its gearing of objective toward security authentication and integrity instead of confidentiality, as main stego intention [5].

This work is going to focus on invisible watermarking type helping ownership authentication proof utilizing the technique presented for counting-based secret sharing [6]. Counting-based secret sharing (CBSS) is simply utilized for this watermarking as identity proofing data-bits scheme. The CBSS data-bits generation takes the owner password (or ID in our watermarking case) and generates shares bits to be distributed and embedded seamlessly within the media-file [7]. The CBSS embedding follow steganography hiding models of data bits as proven to secure not affecting the visibility of the files. Then, at time of verification, these embedded secret bits are recollected again forming the shares. They are combined together providing possible regeneration of the owner password. Therefore, as the owner password can be verified, the watermarking is proving that the copyright claim is authentic announcing proper ownership situation [8]. Interestingly, the counting-based secret sharing strategy allows the correct password regeneration even for not all the shares to be valid, i.e. based on the specification of accuracy intended [9]. This partial share sufficiency gives appealing CBSS research applicability room for watermarking ownership proof, even if

*Corresponding author/Yazışılan Yazar

some tampering has been found occurred to the media-file [10]. Our work considered hiding watermarking within least significant bit (LSB) of the audio samples where we study trade-off between authentication (trustfulness) and security (invisibility), i.e. increasing number of hidden sample bits (1-LSB, 2-LSB, 3-LSB) provided more authentication on the price of transparency security. This research is found important religiously for the Muslims Holy Quran authentic recitation correctness proof as partial alteration percentage needs to be identified clearly to verify recitation correctness.

The paper flow can be ordered by next section, Section 2 providing some related background briefing of watermarking, steganography data hiding and counting-based secret sharing. Section 3 presents the model proposed giving its overview in context of media-file watermarking. Section 4 discuses some remarks behind this audio watermarking approach. Section 5 provides the paper conclusion.

2 Related work

Data hiding for the purpose of information authentication or security involve several areas linking different methods to serve current applications of electronic media files [5]. This research focus is to secure the hidden watermarking data from discovery by unwanted or illegal interference [2]. The objective of this watermarking procedure is to assist verifying copyright authentication [4]. The target aim is on audio watermarking by injecting private data bits to identify the owner authenticity. The work is proposing a watermarking technique that benefits from the lately developed counting-based secret sharing strategies, as will be elaborated next within the coming subsections.

2.1 Watermarking and steganography

Electronic watermarking is the method of inserting specific data within digital media files, such that if moved or copied, the watermarking secret is also affected [5]. This research studies audio watermarking linked to steganography, i.e. directed mainly on securely injecting private e-data in audio cover for authentication. This watermarking research work is directed toward copyright defense applications to avoid or detect unlawful utilization or usage of e-media files [2]. In general, watermarking schemes considerers three main points [4], as briefed below:

- Robustness: hidden data cannot be removed or destroyed,
- Identicality: copyright protected media files should be looking same,
- Safety: unauthorized parties cannot find or tamper the watermarking data.

The linking of watermarking and steganography research objectives can be understood from Figure 1 [11]. Interestingly, watermarking is slightly differentiated from fingerprinting although providing same protection objective as specific security under steganography. In fact, steganography is changing within the media-file by hiding data in such a way that only intended parties are able to detect the hidden through it, as detailed for text steganography in [12] and [13]. In some cases, steganography can serve similar security applications to further cryptography, but in a unique mode as it does not attract attention to itself at all [14].

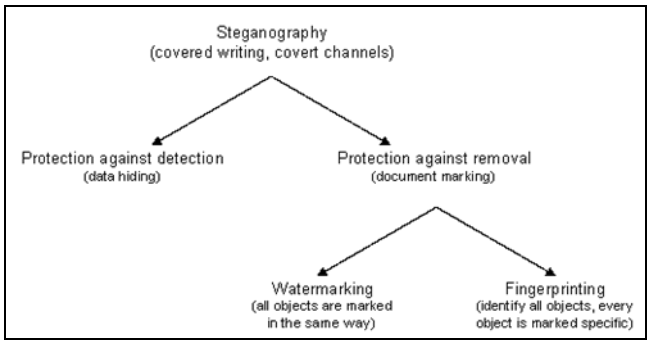


Figure 1. Watermarking within steganography types [11].

2.2 Related audio watermarking

Several related watermarking schemes have been searched within the literature [1]. Some audio works are linked to this research more than others. For example, Liang and Xiang [3] presented adjustable watermarking robust audio-based model with variance statistics. Their work divided all original audio files into frames for statistical histogram computation to be shifted by a hiding key for embedding the watermarking sequence. The work considered histogram shifting inverse operation used for watermarking extraction making the input audio file reinstated afterword as being original. The work can be helpful even if the media file is breached by some audio undesired signals as well as MP3 transformation of 48 Kbps and Gaussian noise of 25 dB. The research [3] testing have revealed the efficacy of the Liang and Xiang innovated structure but needing complex operations not accommodating the audio file being partially corrupted or hacked.

Similarly, Nejad et. al. [15] researched to enhance least significant bit (LSB) methods for audio watermarking based on quantum image security schemes, i.e. suitable for reflected gray code nano communication networks. The work of [15] is considered an improvement to their work of quantum image watermarking of embedding key of the host quantum audio signal [16] as well as [17]. The boosted audio watermarking work of [15] utilized a newly proposed sampling gray images to be scrambled modifying pixel values other than adjusting pixel locations. The twisted pixels image is improved to fulfill the one-dimension audio signal in order to hide the secret watermarking bits within the audio quantum signal via implanting a watermarking password key. Implementation remarks justified the benefit of the improvement schemes acceptable security but found cannot be used for any partial corruption.

Bajpai and Kaur [18] presented a survey on relevant current sound files watermarking procedures highlighting many challenges. Their survey covered algorithms run on dissimilar frequency domain, dimensional fields, and hybrid arena, all serving sound e-audio watermarking. The review study showed several drawbacks raising the main challenges of the audio watermarking which ignited our work of semi complete authentication.

Shuo et al. [8] presented an interesting auto-correction audio watermarking procedure for authentic sound-transformation. Their model considered watermarking to run over compressed version of input audio media hiding secrecy into LSB region. The work suffers from high complexity utilizing the LSB as a parameter within the study explicit mathematical formulations. Also, the work is found limited in the number of LSB layers affecting the total bit layers not to be applicable in all real-life

applications. This research justified the price to be paid against choice variations of LSB levels preferred by diverse application circumstances. This idea of [8] innovated our testing models to involve different number of LSB authentication bits. We considered studying 1-LSB, 2-LSB, 3-LSB, designs as they showed trade-off between authentication (trustfulness) and security (invisibility).

The real challenge to be addressed within this scope proposal is as the audio file is partially corrupted unintentionally or intentionally. Unintentional fractional modifications can be found due to technical or networking reasons. Intentional planned alteration can be found to hinder the copyright ownership or correctness problem as well as religious or political reasons such as holy Quran unauthentic recitation. This issue of partial alteration is our driving force toward this study to involve counting base secret sharing (CBSS) for audio watermarking.

2.3 Counting-Based secret sharing

Counting based secret sharing (CBSS) is considering the digital data as binary bits, i.e. to create its shares from the password (or ID ownership proof) [19]. Its logical shares development procedure relies on replacing specific zeros consecutively to generate original shares. This CBSS method initially considered certain schemes for making shares, as detailed in [6] and modified in [20] and [7] as well as in [14] and [19], i.e. to be adjusted for specific applications and scenarios [21]. For simplicity, the original shares generation process is changing specific one-bit from the password to produce the shadow shares, i.e. converting 1-bit of zero every new run to get another shadow share [6]. Assume as an example, our Password bits: ID=1010 0100, the shadow shares production can provide five shares as following:

ID = 1 0 1 0 0 1 0 0; Sh1: 1 1 1 0 0 1 0 0; Sh2: 1 0 1 1 0 1 0 0

Sh3: 1 0 1 0 1 1 0 0; Sh4: 1 0 1 0 0 1 1 0; Sh5: 1 0 1 0 0 1 0 1

For ID regeneration, the CBSS scheme make parallel sum calculation of entered shares bits. Then, consider the counting summation total linked to k value threshold. If the parallel sum is more than k, the feedback marks value of one, otherwise it preserves zero. This feedback remarking compresses the anticipated ID, as covered thoroughly in [6]. Note that this CBSS arrangement relies on digital bits system pretending ambiguous to provide secure ID against looking at the shadow shares individually [7]. The interesting part of involving CBSS for watermarking is the possibility to regenerate the ID from the shares combining a smaller number of shares based on the condition value k. This k assumption is giving the opportunity for some media-file alteration to be preserving the ownership password ID, which is the real benefit behind this contribution.

The counting-based secret sharing (CBSS) original technique overview is shown in Figure 2 [14].

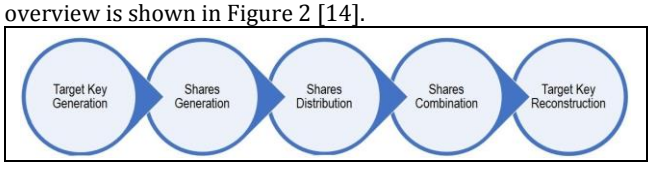


Figure 2. Original counting-based secret sharing overview.

The strategy main steps start by target key generation. Then, producing the shares followed by them distributed. Next, at the construction, the shares are combined and the target key is regenerated again. This work is tuning the original CBSS for utilization within watermarking in semi authentication approach.

To put the contribution clearly, this work is serving audio watermarking ownership copyright authentication focusing on verification challenge when simple tampering occurs, i.e. on the audio multimedia file, which cause difficulty in its copyright proof. This incomplete proof is the novel proposal obtained utilizing counting-based secret sharing but tuned differently for ownership correctness semi-authentication.

3 Proposed audio watermarking

This audio watermarking proposal is intended to utilize counting-based secret sharing (CBSS) system to generate the shares combined as watermarking-bits stream, technically similar in principle to [22] which is for steganography. The watermarking bits stream is then embedded within the audio file for semi-complete verification (semi-authentication), as analogy shown in Figure 3.

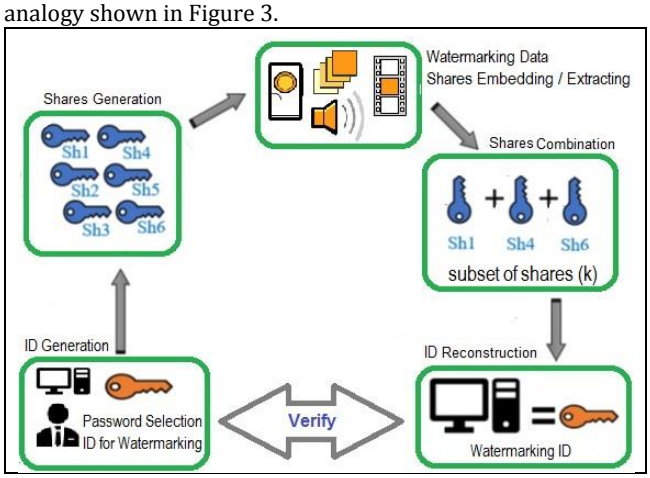


Figure 3. Audio watermarking analogy based on counting-based secret sharing.

The scheme originality starts by asking the user to select the watermarking-ID (password) used within the CBSS system as target key TK, i.e. as the user watermarking password, as main adjustment to random TK generation in [6], as shown in Figure 4. Then, the system automatically produces shares as watermarking-bits stream in specific procedure, known as the 1-bit shares generation phase in [20]. After that comes the watermarking embedding, i.e. after completion of the share's generation as watermarking-bits stream, where to be embedded within the intended cover audio file to store their watermarking bits.

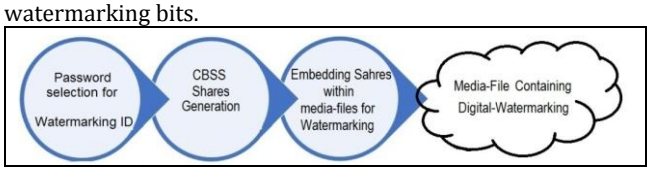


Figure 4. Watermarking audio embedding via CBSS strategy.

This watermarking process consists of embedding the shares, i.e. watermarking-bits, that will be reconsidered at the watermarking-bits (share's) extraction phase for verification [21]. Similarly, this shares extraction process is done partially as not needed for all the audio samples bytes, or accepts some slight alteration in parts of the audio files, but still considered having ownership authentication, which is utilized for this semi-complete verification (semi-authentication). In fact, the system, randomly selects different audio samples, grouped as k

threshold of CBSS, to extract the shares and reconstruct the TK-shadows. This shares extraction phase, only selected (part of all) pixels of watermarked-audio (containing shares), are used via CBSS system to recover the TK-shadows to be verified vs. TK (watermarking-ID), as illustrated within Figure 5. Note that not all shares combination TK-shadows will provide the correct TK making-up the percentage of watermarking verification semi-authentication. The watermarking embedding and extraction processes as well as the simulation strategy are illustrated next.

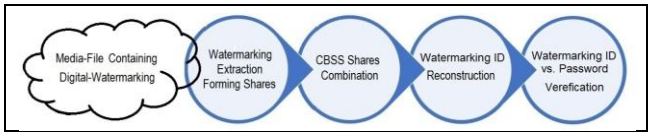


Figure 5. Watermarking audio extraction via CBSS strategy.

3.1 Watermarking embedding

Our proposed watermarking embedding is basically developed from the traditional LSB steganography CBSS lately presented method [23], which generates the shares watermarking bits from a random generator. This proposal generates the watermarking bits stream from combining the shares of CBSS, to allow for partial verification. All watermarking audio embedded bits are to be inserted into LSB specific positions of the cover audio samples bytes as shown in Figure 6. Therefore, the distortion is negligible and will be distributed fairly among all different places of the cover-audio, which is also similar in principle to the matrices spreading of secrets within watermarking research [18]. In general, secret sharing advanced strategies recommend spreading the shadow shares based on the secret data, i.e. to give the required acceptable authenticity [19].

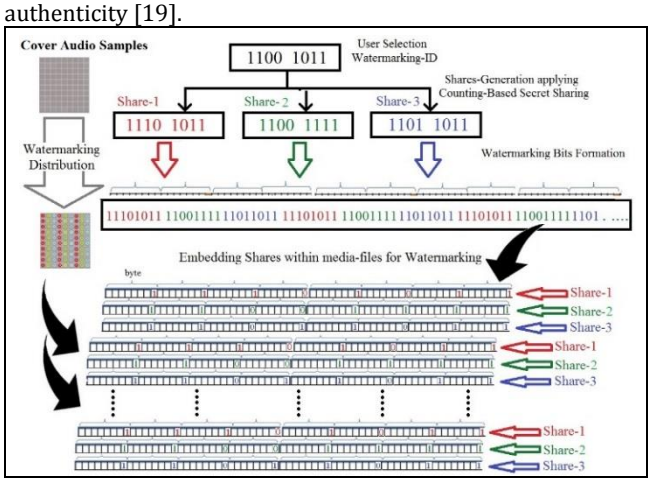


Figure 6. Framework of CBSS watermarking on audio sample.

In this proposed work, the watermarking spreads its hiding over the audio-media files utilizing audio redundancy strategy, as secreting the shadow shares bits generated from CBSS, serving the essential audio security researches justified in [24], [25] and [26] as well as [27],[28] and [29]. This audio watermarking research enhanced more concealed bits in the audio multimedia utilizing many LSBs to advance the construction authentication capacity instead of using only one LSB, as will be shown later in the next section. The research tested on (WAV) audio files, after sampling bytes choosing the tested e-audio in binary, as shown in Figure 7.

To clarify the embedding process, consider audio samples (Figure 7) as the matrix model simple example illustrated in Figure 6. The work is similar in principle to RGB image mixture of red, green, and blue joint in many variation strengths to replicate inclusive color assembly contained 24-bits per pixel [30]. As every RGB pixel contains 3-bytes, the implanting of the watermarking-bits stream is performed within all bytes LSB of the RGB image analogy. This strategy is completely different than the variable length image stego [31] and its high capacity LSB modification [32] benefitting from the analogy of using LSB substitution, PVD, and EMD [33] as well as the adaptive and non-adaptive PVD steganography using overlapped pixel blocks [34].

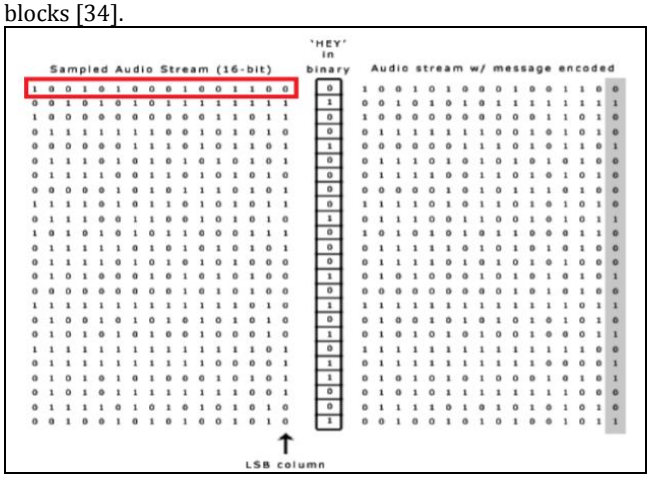


Figure 7. Binary bits audio file sample representation.

Testing our scheme commences by CBSS producing the shares private bits stream based on secret password, pretending the CBSS shadow shares generation process. During this CBSS process, the program takes the Watermarking main password ID to produce the shares sequence that will be hidden within the audio multimedia. The watermarking embedding asks the user to provide original cover audio-file to be represented in binary form. Then, embedding process starts by concealing text bits within the entire audio-file until the watermarking is fully inserted producing the watermarked audio media file.

Testing the proposed model example is shown as a procedure flow graph in Figure 8. The experimentation run on cover sound media named “Bassline” of 3.45 MB in size. The algorithm first generates the intended watermarking secret shares via CBSS. The button “Embed Data” is used to allow the user to control embedding watermarking within the audio file to be holding all the bits of shares sequence. The resulting of concealing the secret data as watermarking provide modified audio file that is marked via watermarking. Note that the shares (watermarking-bits stream) are distributed over the entire audio file in order to spread secrecy among the entire samples space avoiding concentration on the traditional parts, i.e. of the beginning audio file area for embedding. The shares size (as TK Size) affects the distribution of shares among the audio samples bytes in interesting manner, as tested with different sizes in the comparison section. The proposed embedding technique is articulated as briefed in Algorithm 1.

Algorithm 1: Embedding process

1: User select Watermarking-ID (Password) => Representing TK of CBSS.

2: Compute TK-size : size of TK in bits

3: Generate shares via Counting-Based Secret Sharing (CBSS).

4: User select the intended media (cover-audio) for watermarking.

5: Divide audio file via sampling into bytes collection of 8-bits samples representations.

6: Represent all CBSS Shares (generated from TK) in sequence as stream of watermarking bits repeated as total number of sample bytes.

7: Embed watermarking stream bits sequentially as LSB bits within all audio samples bytes.

8: Produce the watermarked audio samples bytes holding watermarking bits steam.

9: End.

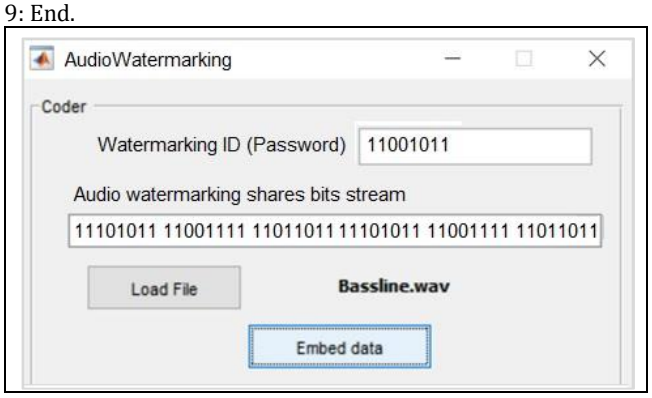


Figure 8. System interface showing the process of concealing secret shares data within audio watermarking.

3.2 Watermarking extracting

For reconstructing TK-shadows combining extracted share keys, the proposed approach run the operation of Algorithm 1 in semi opposite order, to form the embedding process, but not needed on all the audio samples bytes. The system asks for the password (Watermarking-ID) to compute the TK-size. Then, all bytes of the audio samples are divided into 8-bits parts to form groups of samples-blocks. Then, the CBSS reforms TK-shadows by randomly combining several k shares from different random blocks. The TK-shadows are compared to watermarking-ID (password TK) to calculate the ratio of correct TK-shadows vs. TK providing acceptability percentage watermarking semi-authentication, as shown in Figure 9.

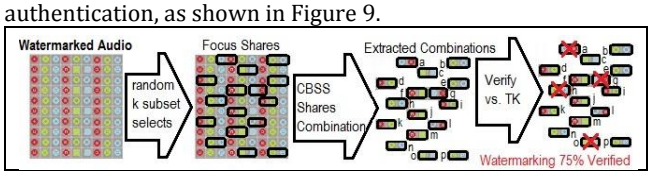


Figure 9. Example of watermarking semi-authentication percentage estimation on audio files.

This part is the interesting unique novelty from using CBSS, which can be benefitable in partial verification as well as helping in reducing the delay for verification as compared to traditional all watermarking bits checking. The proposed CBSS watermarking extracting process is expressed as outlined in Algorithm 2.

Algorithm 2: Extracting process

1: Get watermarked audio file provided by user.

2: Get Watermarking-ID (Password) as TK of CBSS.

3: Compute TK-size : size of TK in bits

4: Divide audio file into bytes collection of 8-bits samples representations.

5: Group audio samples bytes into sampling-blocks of TK-size each.

6: CBSS system selects the 'k' threshold of acceptable number of shares to reconstruct TK-shadows.

7: Randomly select k audio samples-blocks as focus shares for CBSS consideration.

8: Combine every k bytes of samples-blocks separately via CBSS TK reconstruction to represent TK-shadow.

9: Compare all TK-shadow results vs. TK Watermarking-ID to represent percentage of watermarking verification.

10: End.

Figure 9 shows the technical extraction and process applied on the audio samples as an example providing 75% semi-authentication percentage. Figure 10 shows the interface used for testing recovering the watermarking private data bits, that was concealed within our audio example file using this CBSS watermarking scheme. Clicking "Verify Watermarking" of the platform (Figure 10) will be collecting the hidden bits as randomly scanning several LSBs within the watermarked media file combining the data to reconstruct the shares sequences. After that, the shares are joint via CBSS to verify its semi-authentication. The percentage is estimated by the ratio of correct TK values formed from the retrieval CBSS.

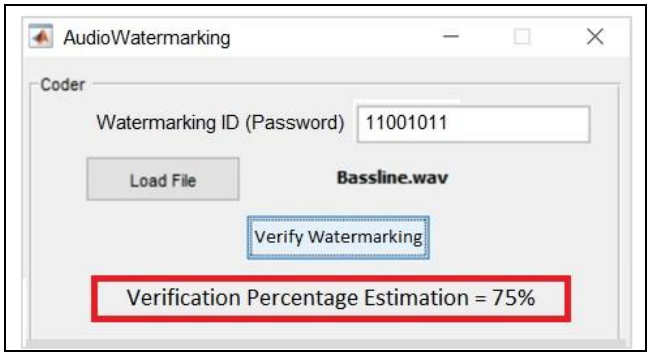


Figure 10. Extracting watermarks verification semi-authentication percentage estimation.

4 Remarks of audio watermarking testing

The presented watermarking semi-authentication of hiding secret data within e-audio has been research tested via MATLAB coding analogy. The MATLAB platform is preferred due to its computation performance and simple visualization as well as its helpful service development tools and clear data analysis capabilities [13]. Furthermore, MATLAB libraries and formulas are well-defined for simulation testing with cooperative manuals and easy overlook assisting researchers while running the implementations of either embedding or retrieving watermarking data of the audio media-files. MATLAB offered us the full facility to use its university access libraries providing immediate entree to many different routines programed by specialists and professionals. Furthermore, MATLAB enjoyed common researcher's publicity giving generous supportive coding and information for educational and academic purposes making it possible to regenerate the experimentations again for further research improvements.

The secret sensitive shares sequence is inserted in 15 dissimilar audio testing files to be studied and compared fairly. This analysis nominated the audio-media files to be variant in sizes covering different options from the PC cover-audios. The

testing compared the consequences of watermarking hiding the shadow shares stream examining the capacity size and secrecy authentication. The work further tested hiding different LSB bits within each audio file, i.e. running diverse LSBs to show top overview remarking of the study. The analysis designated LSBs tested 1-LSB, 2-LSB, 3-LSB to hide the watermarking private shares sequence data bits generating remarks feedback as briefly listed in Table 1. The security and capacity feedback of the watermarked audios showed interesting results because of hiding secrecy in different LSBs as outlined in Figure 11 that will be elaborated later.

Recall Table 1 remarking hiding watermarking secrets on 15 various e-audios. The authentication verification researched secrecy on the audio's media remarked data altered as on the LSB 3 models (1-LSB, 2-LSB, 3-LSB) preference tested, as listed in the Table 1. These hiding capability figures revealed the fraction calculation estimating security and capacity ranges per e-audio media files, i.e. by means of the security formulated using PSNR (Peak Signal to Noise Ratio) based on equation (1), as considered from research [11].

$$PSNR = 20 \log_{10} \frac{MAX}{\sqrt[2]{MSE}} \quad (1)$$

Note that MAX denotes the highest intensity of the assumed resolution within every sample byte, benefitting from image stego studies, such that the MAX value of image case is 255 [13]. Relatively, MSE is estimated as the error square linking the original e-audio cover with the watermarked e-audio [10]. The measurements of MSE is represented by formula (2) to be used for PSNR computations.

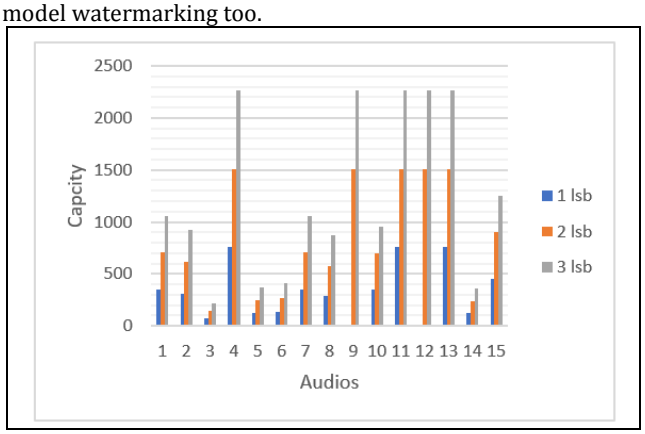
$$MSE = \sum_{i=0}^{allByte} \sum_{j=0}^{allBytes} \frac{(cov(i,j) - hiding(i,j))^2}{m \times n} \quad (2)$$

The capacity watermarking approximation is estimated by the volume of secrecy that can be secured privately within the e-audio media, as illustrated in metric formula (3).

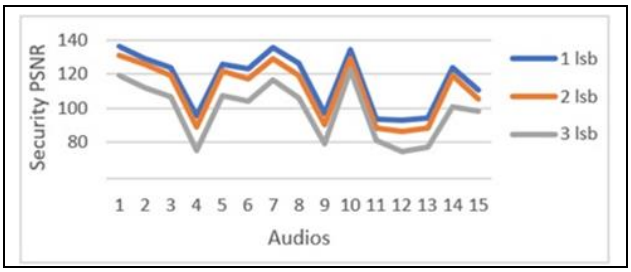
$$capacity = \frac{(number\ of hiding\ bits\ ) \times 8}{number\ of\ bits} \times 100 \quad (3)$$

Considering Table 1 results visualized in Figure 11, remark the dependency of the LSB used on e-audios files available in the PC to sense the secrecy and capacity variations that cannot be predicted. Our testing e-audio watermarking experimentations is displaying different percentages of security results based on the specific watermarking (1-LSB, 2-LSB, 3-LSB) model incorporated. Observe Figure 11, as the LSB model increase in hiding within number of bits of LSB, the security will be reduced, which can be expected as a cost of increasing embedding authentication capacity bits. This secrecy affected the capacity inversely, making the watermarking hidden data size within the e-audio media rise (pretending more authentication) as increasing the LSBs hiding number of bits within every sample byte. Furthermore, the e-audio media file size showed a further variation consequence on security and capacity tested hiding the CBSS shares stream. Note in Figure 11, the sample e-audio "1" of 1-LSB is listing the max watermarking secrecy ratio to imbed private CBSS shares bits. Similarly, consider Figure 12, the audio files: 4, 9, 11, 12, 13, running 1-LSB stego-model is resulting best capacity with acceptable security compared to e-audios 1, and 7, which are giving highest security but reduced capacity, i.e. contrasted with other e-audio media.

The testing watermarking running 2-LSB showed higher capacity of securing authentication watermarking data bits with satisfactory secrecy but lower than that of 1-LSB model. Observe Figure 11, the e-audio "12" is providing the min secrecy ratio to imbed privacy. Watermarking e-audio "1" is the preferred selection to securely hide the CBSS shares bits, conferring to the values of PSNR. It is to be mentioned that e-audio "1" is showing the preferred assumption adopting 3-LSBs model watermarking too.



(a): Capacity (Hiding Capability).



(b) PSNR (Security)

Figure 11(a): Capacity (hiding capability) and (b): PSNR (security) estimation tested for hiding same CBSS shares using dissimilar audios of diverse sizes.

As noticed in Figure 12, the e-audio "8", and "14" are both providing similar security ratios with clear dissimilar hiding capacity estimations. This observation can lead to remark the effect of e-audio media file size on the security PSNR approximation, exactly as the content of the files showed some impact on the security rough calculation, i.e. validating the data reliance and its reputation, as can be detected from the thorough investigation considering Figures 13, 14, and 15.

Hence, remark that our work used 3-LSB watermarking model to enhance the secrets capacity for more authentication watermarking as a development to the commonly used schemes of 2-LSB hiding strategy. In fact, we observed via this research work that the 3-LSB and 2-LSB is providing same level of security preserving adequate watermarking overview remarks, i.e. of trusted concealment from illegal discovery. The key variation of this e-audio watermarking work over earlier comparable studies is the running of semi-authentication involving of CBSS, which further showed watermarking efficiency testing verified by faster verification due to partial confirmations. Interestingly, this work simulated utilizing 3-LSB in securing the watermarking data bits to boost the authentication amount with reflection on the quality of the audio files after the security embedding.

Table 1. Security testing on 15 different audio files using our 3 watermarking models.

Audio Test-File Number	Model 1 (1-LSB)		Model 2 (2-LSB)		Model 3 (3-LSB)	
	Hiding Capability	PSNR	Hiding Capability	PSNR	Hiding Capability	PSNR
1	352.9	136.2	705.9	130.8	1058.8	119.0
2	306.1	129.2	612.2	125.3	918.4	111.7
3	73.1	123.5	146.2	119.2	219.3	106.6
4	756.0	95.4	1,512.0	88.8	2,268.0	75.4
5	123.5	125.4	247.0	121.6	370.5	107.4
6	135.8	122.9	271.7	117.4	407.6	104.2
7	352.9	135.5	705.9	129.2	1,058.8	116.5
8	289.1	126.2	578.2	119.3	867.4	105.7
9	756.0	96.5	1,512.0	90.5	2,268.0	79.3
10	350.8	134.1	700.0	128.8	950.7	122.5
11	756.0	93.4	1,512.0	87.99	2,268.0	81.3
12	756.0	93.1	1,512.0	86.08	2,268.0	74.5
13	756.0	94.3	1,512.0	88.37	2,268.0	76.8
14	120.2	123.5	240.4	119.2	360.5	100.6
15	450.3	110.3	900.6	105.5	1250.0	98.2

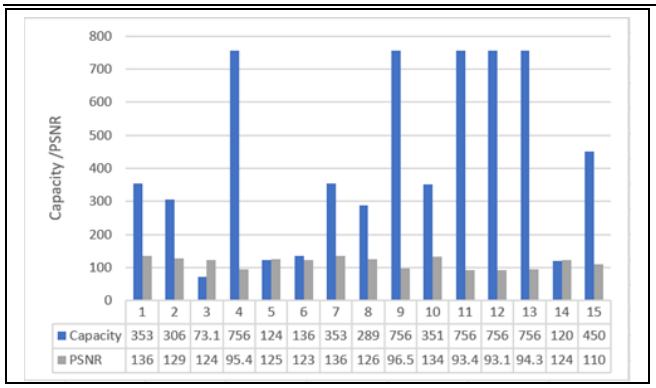


Figure 12. Capacity and PSNR values utilizing 1-LSB watermarking model on different audios.

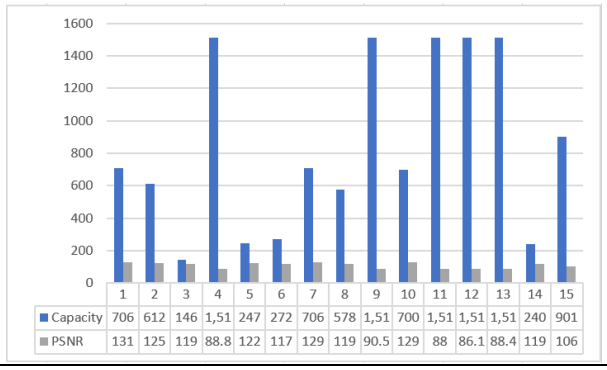


Figure 13. Capacity and PSNR values utilizing 2-LSB watermarking model on different audios.

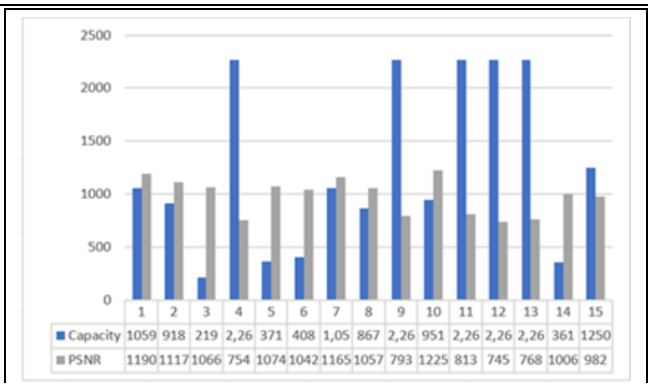


Figure 14. Capacity and PSNR values utilizing 3-LSB watermarking model on different audios.

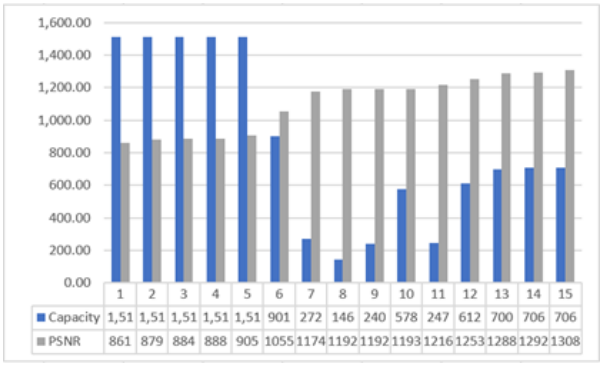


Figure 15. Capacity and PSNR values utilizing 3-LSB model reordered based on PSNR security.

Therefore, considering this semi-authentication research compared to others, we noted the study [26] is involving 6-LSB and 7-LSB to hide sensitive data increasing the capacity of hiding on the price of changing the e-audio media that showed clear noise to it in an unacceptable manner. Based on that, this work preferred not exceeding 3-LSB providing a suitable tradeoff between satisfactory watermarking authentication performance. The work further considered exploring related security authentication works presented in [5] and [9] as well as [22],[30] and [23], as compared to our multibit hiding strategy. The different works [5],[9],[22],[23],[30] run secreting the data assuming 1-LSB, which is very much losing in the hiding capacity as proven to be increasing benefitting authentication as we suggested involving 3-LSB preserving satisfactory security.

Observe again the capacity and security comparison within Figure 11, as showing consistent rising marks in relation to the different LSB models, i.e. 1-LSB, 2-LSB, and 3-LSB. These experimentations are providing variations within selections as based on the audio file used and the user priority as discussed earlier. Therefore, to justify the 3-LSB model preference, we involved a cost function as figure-of-merit to be used for overall approximation, i.e. linking PSNR and capacity, as helping in the selection process. This cost function is understood from the

approximation of area time efficiency similar analysis within the hardware study [35] but in relation to the audio multimedia files, as formula (4).

$$cost = PSNR \times Capacity \quad (4)$$

It is fair to stress mentioning that this cost analysis is just a rough calculation to be used as logical assistant for the selection of appropriate model for the specific audio authentication. This cost estimation can be observed in Table 2 remarking the preferred models choice to be 3-LSB (Model 3).

Table 2. Cost estimation applied on the 15 different audio files using our 3 watermarking models.

Audio Test-File Number	Model 1 Cost (1-LSB)	Model 2 Cost (2-LSB)	Model 3 Cost (3-LSB)
1	48064.98	92331.72	125997.2
2	39548.12	76708.66	102585.28
3	9027.85	17427.04	23377.38
4	72122.4	134265.6	171007.2
5	15486.9	30035.2	39791.7
6	16689.82	31897.58	42471.92
7	47817.95	91202.28	123350.2
8	36484.42	68979.26	91684.18
9	72954	136836	179852.4
10	47042.28	90160	116460.75
11	70610.4	133040.88	184388.4
12	70383.6	130152.96	168966
13	71290.8	133615.44	174182.4
14	14844.7	28655.68	36266.3
15	49668.09	95013.3	122750

5 Conclusion

This work presented a security system of watermarking partial authentication. It is concealing secret data of shares generated from counting-based secret-sharing (CBSS) to allow possible verification semi-authentication. We used CBSS with embedding bits within 1-LSB, 2-LSB, and 3-LSB for watermarking capacity and security variation. The approach was performed and tested via MATLAB platform remarking inspiring results. The scheme masked secret shares bits in the e-audio media file after sampling it into several bytes for the LSB models showing the effect on size and privacy. The models run testing experimentations sensing the security of 1-LSB, 2-LSB, and 3-LSB schemes in attractive manner. The study inspected the connection and impact between the shares secret data bits to be hidden in the audios file and the e-audio files features on the testing platform. The experimentations run over fifteen different sizes audios with three variant models offering stimulating outcomes effecting tradeoff of security vs. capacity.

As future work, we suggest proportion testing and analysis based on quality index computation. The work can involve improvements adopting this semi-authentication technique on video files as of their business need for proper verification. The research can further increase its complexity using cryptography to test combining the study with different symmetric and asymmetric algorithms involving elliptic curve encryption [36] and hash multi-threading parallelization [37]. The research can further be tested for images watermarking as well as different languages audio sensing its effectiveness in real life different IoT applications [38] and privacy needs [39], hoping to find new directions of related open research contributions.

6 Acknowledgment

Thanks to Umm Al-Qura University for the motivation.

7 Author contribution statements

All work is conducted by Adnan GUTUB whom declare work originality and not considered to be published in other media.

8 Ethics committee approval and conflict of interest statement

No need for permission from ethics committee for the article prepared. There is no conflict of interest in the article prepared.

9 References

[1] Gutub A. "Watermarking ımages via counting-based secret sharing for lightweight semi-complete authentication". *International Journal of Information Security and Privacy (IJISP)*, 2022. http://doi.org/10.4018/IJISP.2022010118.

[2] Almazrooie M, Samsudin A, Gutub A, Salleh MS, Omar MA, Hassan SA. "Integrity verification for digital Holy Quran verses using cryptographic hash function and compression". *Journal of King Saud University-Computer and Information Sciences*, 32(1), 24-34, 2020.

[3] Liang X, Xiang S. "Robust reversible audio watermarking based on high-order difference statistics". *Signal Processing*, 2020. http://doi.org/10.1016/j.sigpro.2020.107584.

[4] Gutub A, Ghouti L, Amin A, Alkharobi T, Ibrahim MK. "Utilizing extension character 'kashida' with pointed letters for arabic text digital watermarking". *International Conference on Security and Cryptography (SECRYPT)*, Barcelona, Spain, 28-31 July 2007.

[5] Gutub A, Al-Haidari F, Al-Kahsah K, Hamodi J. "e-Text watermarking: utilizing 'kashida' extensions in arabic language electronic writing". *Journal of Emerging Technologies in Web Intelligence (JETWI)*, 2(1), 48-55, 2010.

[6] Gutub A, Al-Juaid N, Khan E. "Counting-Based secret sharing technique for multimedia applications". *Multimedia Tools and* Applications, 78(5), 5591-5619, 2019.

[7] AlKhodaidi T, Gutub A. "Trustworthy target key alteration helping counting-based secret sharing applicability". *Arabian Journal for Science and Engineering*, 45, 3403-3423, 2020.

[8] Shuo Li, Zhanjie Song, Wenhuan Lu, Daniel Sun, Jianguo Wei. "Parameterization of LSB in self-recovery speech watermarking framework in big data mining". *Security and Communication Networks*, 2017. http://doi.org/10.1155/2017/3847092.

[9] Gutub A, Al-Ghamdi M. "Hiding shares by multimedia ımage steganography for optimized counting-based secret sharing". *Multimedia Tools and Applications*, 79(11), 7951-7985, 2020.

[10] Gutub A, Alaseri K. "Hiding shares of counting-based secret sharing via arabic text steganography for personal usage". *Arabian Journal for Science and Engineering*, 45(4), 2433-2458, 2020.

[11] Richard Popa. An Analysis of Steganogrphic Techniques. Master Thesis, Department of Computer Science and Software Engineering, Faculty of Automatics and Computers, The Politehnica University of Timisoara, 1998.

[12] Gutub A, Fattani M. "A novel arabic text steganography method using letter points and extensions". *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 1(3), 502-505, 2007.
[13] Al-Nofaie S, Gutub A, Al-Ghamdi M. "Enhancing arabic text steganography for personal usage utilizing pseudo-spaces". *Journal King Saud University-Computer and Information Sciences*, 2019.
[14] Gutub A, Alkhodaidi T. "Smart expansion of target key for more handlers to access multimedia counting-based secret sharing". *Multimedia Tools and Applications*, 2020. https://doi.org/10.1007/s11042-020-08695-y.
[15] Nejad MY, Mosleh M, Heikalabad, SR. "An enhanced LSB-based quantum audio watermarking scheme for nano communication networks". *Multimedia Tools and Applications*, 79, 26489-26515, 2020.
[16] Nejad MY, Mosleh M, Heikalabad SR. "An LSB-Based quantum audio watermarking using MSB as arbiter". *International Journal of Theoretical Physics*, 58, 3828-3851, 2019.
[17] Nejad MY, Mosleh M, Heikalabad SR. "An enhanced LSB-based quantum audio watermarking scheme for nano communication networks". *Multimedia Tools and Applications*, 79, 26489-26515, 2020.
[18] Bajpai J, Kaur A. "A literature survey-various audio watermarking techniques and their challenges". *IEEE International Conference-Cloud System and Big Data Engineering (Confluence)*, Noida, India, 14-15 January 2016.
[19] Al-Ghamdi M, Al-Ghamdi M, Gutub A. "Security enhancement of shares generation process for multimedia counting-based secret-sharing technique". *Multimedia Tools and Applications*, 78, 16283-16310, 2019.
[20] Gutub A, Alaseri K. "Refining Arabic text stego-techniques for shares memorization of counting-based secret sharing". *Journal King Saud University-Computer and Information Sciences*, 2019. https://doi.org/10.1016/j.jksuci.2019.06.014.
[21] Gutub A, Al-Qurashi A. "Secure shares generation via m-blocks partitioning for counting-based secret sharing". *Journal of Engineering Research*, 8(3), 91-117, 2020.
[22] Gutub A, Al-Ghamdi M. "Image based steganography to facilitate ımproving counting-based secret sharing". *3D Research*, 2019. http://doi.org/10.1007/s13319-019-0216-0.
[23] AlKhodaidi T, Gutub A. "Refining image steganography distribution for higher security multimedia counting-based secret-sharing". *Multimedia Tools and Applications*, 2020. http://doi.org/10.1007/s11042-020-09720-w.
[24] Deshmukh R, Deshmukh P. "4 Layer enhanced security for audio signals using steganography by modified lsb algorithm and strong encryption key". *International Journal of Advanced Research in Computer Science*, 2(2), 492-495, 2011.
[25] Ravali S, Neelima P, Sruthi P, Sai Dileep P, Manasa B. "Implementation of blowfish algorithm for efficient data hiding in audio". *International Journal of Computer Science and Information Technologies*, 5(1), 748-750, 2014.
[26] Asad M, Gilani J, Khalid A. "An enhanced least significant bit modification technique for audio steganography". *IEEE International Conference on Computer Networks and Information Technology (ICCNIT)*, Abbottabad, Pakistan, 11-13 July 2011.
[27] Shaikh A, Solanki K, Uttekar V, Vishwakarma N. "Audio steganography and security using cryptography". *International Journal of Emerging Technology and Advanced Engineering*, 4(2), 317-318, 2014.
[28] Padmashree G, Venugopala PS. "Audio steganography and cryptography: Using LSB algorithm at 4th and 5th LSB layers". *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(4), 177-181, 2012.
[29] Saurabh J, Ambhaikar A. "Audio steganography using RPrime RSA and GA based LSB algorithm to enhance security". *International Journal of Science and Research (IJSR)*, 1(2), 62-65, 2012.
[30] Gutub A. "Pixel ındicator technique for RGB image steganography". *Journal of Emerging Technologies in Web Intelligence (JETWI)*, 2(1), 56-64, 2010.
[31] Swain, G. "Digital image steganography using variable length group of bits substitution". *Procedia Computer Science*, 85, 31-38, 2016.
[32] Swain, G. "High capacity ımage steganography using modified LSB substitution and PVD against pixel difference histogram analysis". *Security and Communication Networks*, 2018. https://doi.org/10.1155/2018/1505896.
[33] Pradhan A, Sekhar K, Swain G. "Digital ımage steganography using LSB Substitution, PVD, and EMD". *Mathematical Problems in Engineering*, 2018. https://doi.org/10.1155/2018/1804953.
[34] Swain G. "Adaptive and Non-adaptive PVD steganography using overlapped pixel blocks". *Arabian Journal of Science and Engineering*, 43, 7549-7562, 2018.
[35] Gutub A. "Merging GF(p) elliptic curve point adding and doubling on pipelined VLSI cryptographic ASIC architecture". *International Journal of Computer Science and Network Security (IJCSNS)*, 6(3A), 44-52, 2006.
[36] Bin-Hureib E, Gutub A. "Enhancing medical data security via combining elliptic curve cryptography with 1-LSB and 2-LSB image steganography". *International Journal of Computer Science and Network Security (IJCSNS)*, 20(12), 232-241, 2020.
[37] Abu-Hashem M, Gutub A. "Efficient computation of Hash Hirschberg protein alignment utilizing hyper threading multi-core sharing technology". *CAAI Transactions on Intelligence Technology*, IET (IEE)-Wiely, 2021. http://doi.org/10.1049/cit2.12070.
[38] Shambour MK, Gutub A. "Progress of IoT Research Technologies and Applications Serving Hajj and Umrah". *Arabian Journal for Science and Engineering*, 2021. http://doi.org/10.1007/s13369-021-05838-7.
[39] Shambour MK, Gutub A. "Personal privacy evaluation of smart devices applications serving hajj and umrah rituals". *Journal of Engineering Research*, 2021. http://doi.org/10.36909/jer.13199.