Transparent Authentication Methodology in Electronic Education

Nawfal F. Fadhel[*1], David Argles[2], Richard M. Crowder[3], Gary B. Wills[4]

Electronics and Computer Science,

University of Southampton,

Southampton, UK.

[1]nff1g08@ecs.soton.ac.uk, [2]da@zepler.net, [3]rmc@ecs.soton.ac.uk, [4]gbw@ecs.soton.ac.uk

Received 20 January 2014; Accepted 26 March 2014; Published 11 June 2014

Abstract

In the context of on-line assessment in e-learning, a problem arises when a student taking an exam may wish to cheat by handing over personal credentials to someone else to take their place in an exam, Another problem is that there is no method for signing digital content as it is being produced in a computerized environment. Our proposed solution is to digitally sign the participant's work by embedding voice samples in the transcript paper at regular intervals. In this investigation, we have demonstrated that a transparent stenographic methodology will provide an innovative and practical solution for achieving continuous authentication in an online educational environment by successful insertion and extraction of audio digital signatures.

Keywords

Transparency; Authentication; E-learning; Steganography

Introduction

In today's e-learning classroom, virtual exam or any form of virtual presence, it is difficult to confirm personal identification in a virtual session, simply because we cannot identify who is sitting on the other end (Agulla et al. 2008). It's true we have the concept of classical authentication to prove a claim of identity (Burrows et al, 1989). This is a concept, which is designed to protect a person's identity; it is mature and well developed in information technology today. However, while the authentication process was designed to protect personal identity, this situation is reversed in an e-learning situation (Chou et al. 2005); the users will sometimes be willing to exploit the protocol for the purpose of cheating, making them an accomplice by falsifying information or giving information to a person who will help them to pass an on-line exam. In Apampa et al (2009) and Agulla et al. (2008) work has demonstrated a solution for the previous scenario by using continuous authentication, a concept which states *"a user will be authenticated with a reasonable frequency over a period of time to achieve proper monitoring procedures to mimic the manual authentication procedure"*. Note that when Apampa, et al (2009) mentioned *"manual authentication"* the authors are actually referring to the physical process of on-going invigilation, not just the initial process of authentication. Current monitoring solutions are based on mutual trust between student and invigilators.

We believe this procedure places a burden on the authentication process because the only way we can validate authentication is through people who are considered the weakest link in computer security. We can overcome some issues in human behaviour, but not all (Chan et al. 2009; Sasse at al 2001).

There are a number of proposed solutions to the continuous authentication problem. Previous solutions introduced a mild to heavy authentication process and are not entirely user-friendly because of their intrusive behaviour, for example fingerprint scanning every five minutes or sitting still for the biometric to be taken (Agulla et al. 2008). The weight of the authentication process may cause an intimidating atmosphere, affecting the morale of the exam participant, or introducing a hesitant participation in an e-lecture or remote brainstorming session in web seminars. In this paper, we present a non-intrusive authentication protocol that takes advantage of human computer interaction using speech as an authentication factor, the same interactions that the user uses to navigate and answer questions, and therefore not interrupting the user. This confirms presence by using voice matching through a virtual session within a frequency of

interactions over time within an acceptance threshold in the system. Our solution addresses the need for educational institutions or e-learning providers to act transparently towards the general public. For example if we secure an exam transcript electronically, we are required to make copy of the document available if requested, and that is transparency according to Robison et al (2007).

Finally we have chosen steganography to use for secure data encapsulation for data transfer. So we propose a transparent authentication that is defined as an efficient lightweight authentication procedure to confirm ongoing availability behind an electronic learning station with minimum effort from the receiving end in the educational process (e-learning/e-exams) via stenographic encapsulation.

E-learning

Electronic learning or E-learning is a concept that uses a computerized system to deliver educational material. E-learning is becoming very popular because people like the idea of location-free learning especially in this day and age, where learning has to fit our hectic life style. Or in other instances people may require training that is provided by an educational body in another country (Rovai 2001). To have a better understanding of the problem we explain the different types of e-learning environments and material variations in the next sections.

E-Learning and E-Assessment Environment

When we think about e-learning and e-assessment we have different approaches dealing with the situation. E-learning is different from e-testing because of the environmental procedures. In the e-learning process, the emphasis is on the delivery of educational material and on contributing in the lectures and on-line classes (Fadhel, et al 2011). Therefore e-assessment is an assessment process of a taught course regardless of whether the teaching method was on-line or in class teaching (Ssemugabi et al 2007). We have categorized electronic approaches to learning and testing procedures into the following categories:

E-Assessment: Computer based test (CBT), Internet based test (IBT), Web based test (WBT)

E-Learning: Computer based learning (CBL), Internet based learning (IBL), and Web based learning (WBL)

E-learning Material Variations

The nature of the educational material is varied and depends on the academic teaching methods and scientific content (Fadhel et al, 2011). We will summarize the variation in two sections, the exam based material and the learning based material as illustrated below.

Exam based material: Multiple-choice questions, Essay questions, Lab questions**.**

Learning based material: Power point presentation, Video presentation, Webinar Session, Formative/ summative assessment methods.

When we are working on finding solutions in e-learning, we need to build on current designs of learning material. By that we mean, instead of building our own standards of electronic education material we decided to build for current educational material. Since the topic of this paper is the authentication process in e-learning under the educational system we will not go into details of variation of educational material and will use a copy of an exam paper for testing the proposed authentication technique.

Steganography

Steganography is the art of hiding information in ways that prevent the detection of hidden messages, (Johnson and Jajodia 1998; Artz 2001). In steganography the messages are hidden in plain sight and can only be found when we know where to look.

This is the most common definition for steganography that is mostly used in textbooks and research papers. As indicated above the message itself is kept hidden. However, with the current techniques for cryptanalysis, we can prove with acceptable accuracy that the cover medium has been exposed to manipulation. By cover medium we mean the data carrier for the hidden message see (Zhou and Hui 2009; Abolghasemi et al. 2008; Zhi-ping et al. 2007). Now the use of security procedures is a requirement in today's electronic presence, and when we consider that fact with the definition of steganography, we will notice a conflict. The conflict is: the definition states that the presence of message is hidden while our model of authentication dictates that we must use transparency and disclose the fact that there is a security procedure occurring. In other words we cannot say transparent steganography because it defeats the purpose of data hiding. When steganography was first designed, hiding the data was its source of security. Since disclosure of the fact that there exists a hidden message is a must in ensuring transparency, we need to modify the current

steganography, not discard it. The use of steganography has its benefits and advantages. We believe it deserves a second look and it has room for improvement. To build a strong base for our claim we state the benefits and advantages:

- Digital Watermarking (Katzenbeisser and Petitolas 2000): is a process of adding or embedding information into a digital medium to prove its origin and protect the intellectual property (Lin et al. 2008).
- Digital Signature Authentication (Sharp 2001): a digital signature has the same legal status as a hand signature but is constructed using digital means to render it immune to counterfeiting.
- Digital Signature (Sharp 2001): is used in signing a confidential document and is irrefutable by the originator and receiver of the message.
- Digital Linkage and Storage (Johnson and Jajodia 1998): That can be achieved by embedding information into digital media, for example we can insert information like personal or medical record into a personal image or photo.

Transparent Steganography

We take the classic view of steganography a step further and a redefined model is required. We integrate the use of cryptographic keys to achieve security then introduce data encryption into steganography to prevent cryptanalysis, and that it is unique. This is because the cryptographic keys scheme is performed on both the hidden data and the cover medium while encryption is only applied to the hidden data.

There is previous work undertaken by Sharp (2001) which proposes the use of public key encryption (cryptographic key scheme). Our model has an added function and purpose.

Firstly we have converted the use of steganography from a method for securing data to a method for encapsulating the data and acts as data storage without using additional size depending on the amount to be embedded into the storage, then securing the data to be hidden. The stenographic procedure acts as an encapsulation to the hidden data and a cryptographic key secures this encapsulated data. Second, we added encryption to steganography by manipulating the hidden data, not the cover medium in the data preparation step. This acts as a counter measure to stenographic detection (Zhou and Hui 2009; Abolghasemi et al. 2008; Zhi-ping et al, 2007)

Secure steganography

We will now take the classic view of steganography aside and answer the question, what does it mean to have secure data? Secure protected data is electronic storage protected by a cryptographic key as previously discussed by Sharp (2001); the key is a main component in retrieving the secure data from the digital storage (Sharp 2001). First, we have two components. The cover medium will serve as a storage medium and include a key to secure the data. Second, we have a procedure in which the key is used to lock and unlock the data. Through this concept, data security is achieved.

Encrypted steganography

This is a simple question of why do we need to encrypt an existing security protocol and the reason is because of the advanced method mentioned in Zhou and Hui (2009), Abolghasemi et al. (2008), Zhi-ping et al. (2007) It is relatively easy to detect data manipulation and therefore it is relatively easy to extract the hidden information (Zamani et al. 2009). It is similar to sending user name and password in plain text in a security session. We have two reasons for incorporating this concept into steganography. Firstly, one of the benefits of steganography is Digital Linkage and Storage. Since we will use it for data storage, we expect that it will be exposed to malicious attacks to extract the personal data, thus we need a way to secure it. Second, since there are many advanced methods mentioned in Zhou and Hui (2009), Abolghasemi et al.(2008), Zhi-ping et al. (2007) to detect changes in digital media and indicate the usage of stenographic techniques by malicious attackers, we think it is a good idea to incorporate the encryption into our scheme of steganography to prevent cryptanalysis as discussed by Wang et a (2004). Even if the malicious attackers found out that the media contains hidden data (audio medium stream) and they were able to extract the data they cannot decipher its contents without the key, which contains the encryption sequence.

Transparency in Education and Academic Integrity

Transparency or openness is a concept of exposing information to the public. Transparency is a concept studied in social science and it differs from the beholder's point of view, whether it was a user target, organization (Henriques 2007) or a social group

(Robison and Tanimoto 2007). We believe integrating the transparency concept into the Electronic education will make the education process more user-friendly. Thus building a model with transparency as a foundation for the design will target the right solutions to the authentication process in e-learning.

Transparency in Education

Organizational transparency (Robison and Tanimoto 2007) is a must in an educational framework, and we expect the organization to behave ethically. Actions by students should not be restricted unless they act beyond the boundary of the law. Students must feel free to express themselves without the feeling of being monitored. When we have students under constant surveillance it will introduce an intimidating atmosphere (Fadhel, et al 2011), while other studies have produced results that state when students are given freedom and more space they will be more productive (Rovai 2001).

Transparency and Academic Integrity

According to Bingham (2008) "*Target transparency aims to reduce specific risks or performance problems through selective disclosure by corporations and other organizations. The ingeniousness of target transparency lies in its mobilization of individual choice, market forces, and participatory democracy through relatively light-handed government action.*" The statement above is a generalization of the security statement in the context of transparency. The disclosure of secure information must have two sides, first we need to ensure that we can authenticate the information and its source so we can remedy disinformation, and by disinformation we mean falsification of information or stealing copyrighted material and posing as the originating source. The second side is that the mechanism of the disclosure must remain secret. In other words, security procedures by themselves are not transparent but their actions are. In a sense we protect the interest of the students and education board to ensure their transparency through providing security. Users will be able to use the system freely without the fear of the theft of their identity or intellectual property.

Shortcomings in Computer Based Assessment for E-learning Candidates

When we think of e-learning or online exams, we immediately think that it will be easy to bypass most of the security procedures because of a lack of observational procedures. In most cases this is true with the exception of exam centres (which require supervision) or other institutions that are deployed for monitoring technologies purposes. The following statements point to the main issues in today's e-learning.

- Misplaced trust in individuals, such that the students are trying to cheat and invigilators being too lenient and sympathetic to students, which has a negative impact on exam results (King, Guyette, and Piotrowski 2009).
- A great weight of the authentication procedures are manual and not computerized and this not only affects the authentication process but also cripples anonymity (King, et al 2009).
- Lack of friendliness in the exam environment due to the invigilator's presence or the burden imposed by the authentication procedure (Agulla et al. 2008).
- Shyness of people in lectures when their identity is exposed which results in lessened participation (Agulla et al. 2008).

We know that these points are valid for today's approaches to e-learning (Agulla et al. 2008; King, Guyette, and Piotrowski 2009; Rovai 2001)and we also know that the impact is proportional to the educational status promoted by these exams or electronic materials. This means the higher the status rewarded by the education materials, the higher the chance of people trying to overcome the system.

Transparent Authentication

According to Burrows, Abadi, and Needham (1989), Authentication is the process of proving the origin of an object, or proving personal identity. We take this definition and apply it to computer science and the result is virtual presence on an electronic system as discussed by Leite and Cappelli (2010), which encapsulates your information and forms identifiable attributes of a person or an object within the system.

Transparent Authentication means that the authentication procedures are publicized while the inter-workings of the security procedures are kept secret. So in order to have a secure transparent system there are several requirements that need to be met. First, the protocol must be transparent. Second, the protocol needs to be secure and the third requirement is the need for data encryption to be resilient to cryptanalysis techniques. The type of the authentication process can be either singular access (conventional authentication) or continuous to prove

availability.

Authentication in Continuous Presence

Due to the demand of the e-learning education process, the user is required to be continuously present (Apampa, et al2009) behind the computer when taking exams on-line. We need to formulate a process protocol for continuous authentication as illustrated in step two in Fig 1. Previous attempts to solve this problem placed a heavy burden on users because of the frequency demand of authentication. The same problem was described by Matsumiya et al. (2003). We believe our model will achieve that goal efficiently because the use of non-intrusive authentication procedures will make our model feel lightweight to the user by reducing the effort needed to authenticate, as shown by step two in Fig .1. This process will give an incentive for the user to interact with the electronic system since it is a lightweight authentication protocol.

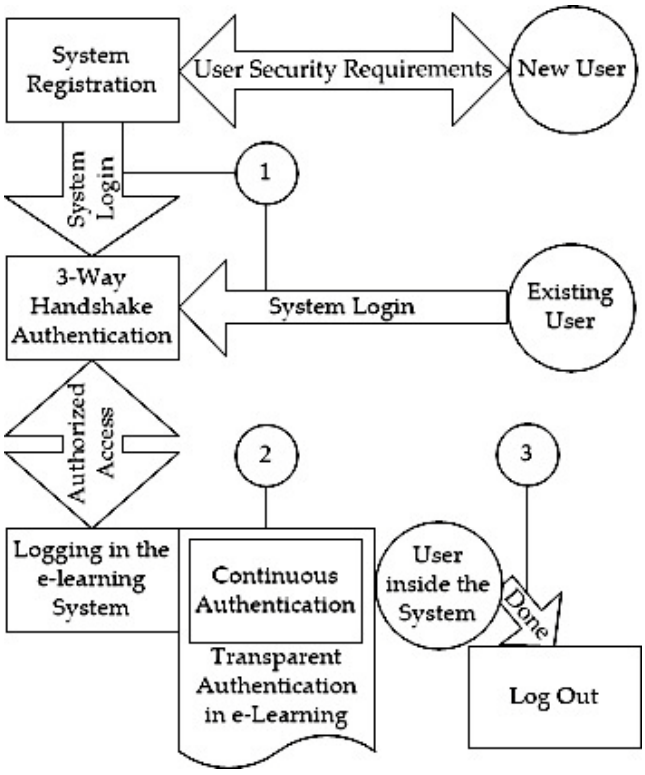


FIG 1. E-LEARNING MODEL WITH THE APPLICATION OF CONTINUOUS AUTHENTICATION METHOD, SHOWING THREE USER INTERACTIONS

Authentication in Identity Proofing

Personal authentication is established by providing the appropriate credentials to prove that you are whom you claim to be. This point shown as step one in Fig. 1, Also it is used in step three to indicate that the user is no longer connected. This process is a typical authentication procedure that is used frequently in everyday electronic systems. In this paper we will not go into inter-working of this protocol as it's beyond our scope of research and has been discussed previously in Burrows, Abadi, and Needham (1989).

Rationale

The rationale behind the approach of using steganography is to add to the computer assisted assessment process, and specifically the authentication component in the process, a method that is less intrusive but also secure. To enable the model to satisfy transparency, and the authentication requirement in e-assessment we use steganography as a data encapsulation technique that is able to carry both data and security protocols. The encapsulated data used in the authentication process is captured using voice samples where the possibility was previously discussed by Skopin (2010); these identification factors are transparent and non-intrusive to students.

Benefits of Transparent Authentication

According to Rovai (2001) they theorized that there are four components to a classroom community; Spirit, Learning, Interactions and Trust. We agree with Rovai (2001) and Lucking's principles and believe that if these conditions are accommodated in the E-learning design, we can achieve a superior learning experience.

- Easing of the authentication process With Spirit: Spirit is the feeling of belonging, acceptance and recognition. These feelings are considered somewhat fragile and easily affected; if we bombard the process with heavy authentication it will break the Spirit component in the classroom community.
- Lowering the intimidating atmosphere with Learning: Learning is the feeling of knowledge and personal intelligence and this feeling can be bullied from individuals and educational systems.
- User-friendly interaction with student Interactions: Interaction is the feeling of closeness and mutual benefit or in other words happiness to participate in a task or in our case a classroom.
- Added security through the use of security keys, cryptography and steganography with Trust: Trust is the feeling of personal security on an emotional level and that feeling is crucial. Because it leads to a willingness to participate within a community that a person feels the sense of belonging.

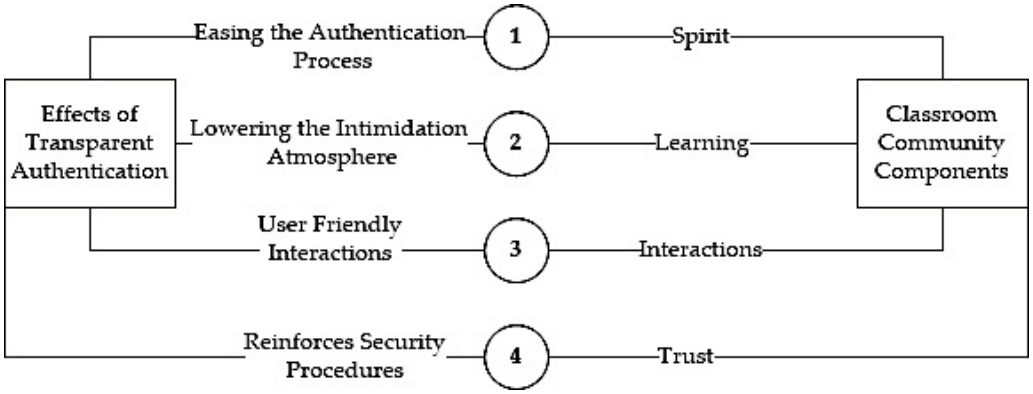


FIG 2 PROPOSED FOUR-LEGGED MODEL OF STEGANOGRAPHY FITS PERFECTLY WITH VALUES OF E-LEARNING.

Methodology

The result of our efforts to solve the shortcomings in e-assessment and e-learning courses has resulted in the construction of a transparent authentication protocol. The user will sit behind a computer and a microphone, and for some tasks the user will need to interact with the learning environment using speech to do common tasks such as turning pages or solve questions, where the user's speech will be used to verify the user's identity. By using the concept of continuous authentication in a transparency framework within the area of e-assessment and achieving it through redefining stenographic techniques and constructing a new protocol, we have fulfilled the requirements and specification of our e-learning model. The transparent authentication protocol operates as continuous presence authenticator using voice identification through interactions between the user and the electronic system. This then encapsulates the data to comply with our security and transparency requirement. Steganography will act as data encapsulation technique, the encapsulated data will be used in authentication through voice identification and the use of the procedure is both transparent to students and educational institutions alike. The user will be notified before a class or exam that voice identification will be used for authentication and the voice interaction will serve in authenticating the student and answering questions. Previous stenographic approaches for audio mediums has been explored by Kumar (Kumar 2007) for copyright protection and for hiding human speech by Skopin et al. (2010) and Zamani et al. (2009).

Fig. 3 shows the data encapsulation phase in which the voice data is embedded in image cover medium. The encoding process requires pre-processing on voice and image data, in which the image data is deconstructed into red, green, blue layers. Voice data is merged with a cyclic redundancy check and then segmented into three data sets. The data set can be customized to the desired bit size ranging from (1-7), and then the data set will be embedded into an image layer occupying the least significant bits in an image layer for example red. Examples of this approach are demonstrated by Chang in (Lie and Chang 1999) and (Chang, Hsiao, and Chan 2003).

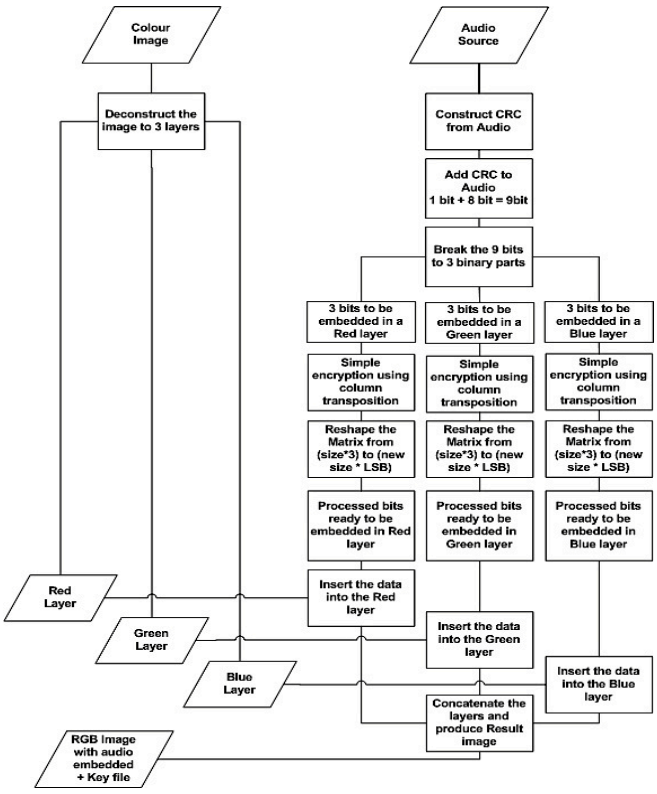


FIG. 3 THE ENCODING PROCESS

Fig. 4 an example of bit replacement on binary-decimal data, where we are using the 3 least significant bits of the image and replacing them with the processed data set with the same size. The resulting quality of the encoding process depends on the number of least significant bits used.

As illustrated in Fig 5, the decoding process will start by extracting the encrypted data from the transfer

medium with the image samples using the cryptographic key. The cryptographic key holds values, which include the size of matrix to be extracted (length and width). We use a function to extract the hidden data from the three-layered matrix by deconstructing it first to three smaller matrices. Then the data is reshaped and rearranged according to the value found in the key in each layer and the last step is to remove the error correction and produce the output.

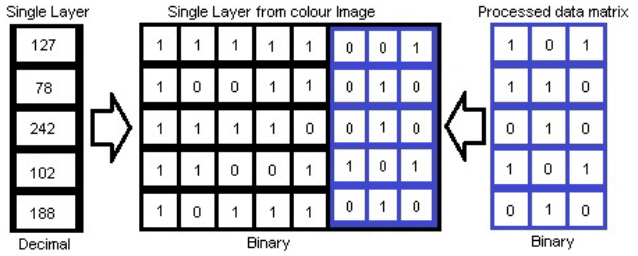


FIG 4 BIT REPLACEMENT OF BINARY DECIMAL DATA

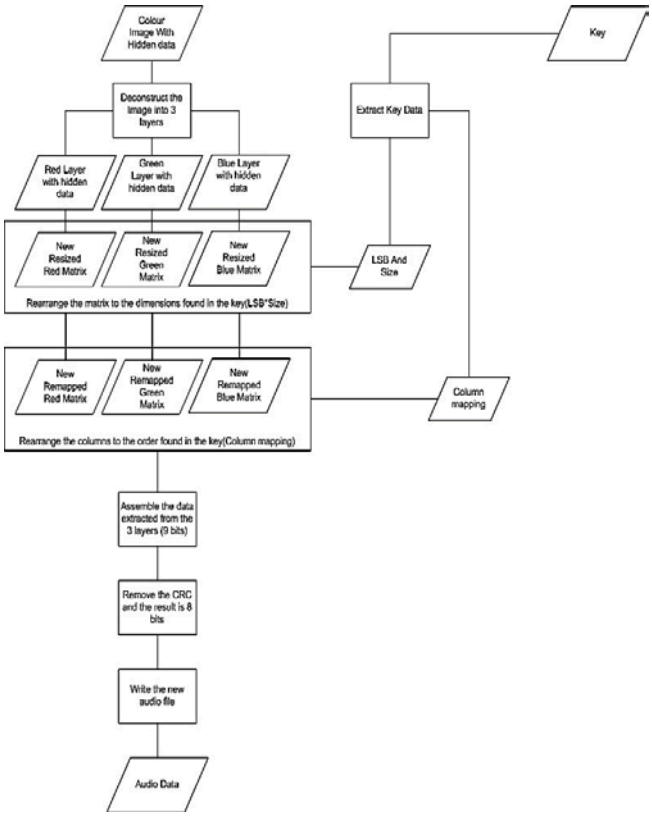


FIGURE 5 THE DECODING PROCESS

The Results

The aim of this experiment is to test the stenographic capacity of the transfer medium, in this case the student's exam script. For our research we have recorded 240 tests in Tables 1 and 2. These also include countless tests performed on colour and text images. We will demonstrate the result of our research. The inputs were described in material and content. The cover medium inputs are image material, And the content are either text or pictorial images. The hidden data is speech audio data and the contents are a few common English words such as numbers and commands. The test samples were available using the Matlab file exchange library

Least Significant Bit data comparison

Table 1 presents the results of 140 tests performed on an image containing 965594 pixels samples, with twenty audio samples for different words. It is clear when using a LSB value of one we have the highest number of samples used in the image, as the values of LSB values increases so the number of the samples needed, will decrease. The purpose of this test is to show data usage in an image, for example if we look at audio sample 'dial' which is the highest value sample we can hide it nine times with some unused samples left and that is only for using LSB - 1, or 19 times for using LSB - 2 but this variation is not fixed. In case of using LSB-1 or LSB-2 it is visually undetectable with the naked eye [27, 28] that proves we have more than enough space to use for hiding speech data. If we needed to use a smaller image we will have less data samples that leads to lower the number of audio samples to be hidden, an efficient balance could be reached once we have specific information of the nature and size of the cover medium and hidden data.

TABLE 1 NUMBER. OF PIXELS NEEDED TO HIDE SPOKEN WORDS

LSB [1]Audio	LSB-1	LSB-2	LSB-3	LSB-4	LSB-5	LSB-6	LSB-7
One	81420	40710	27140	20355	16284	13570	11632
Two	98046	49023	32682	24512	19610	16341	14007
Three	83436	41718	27812	20859	16688	13906	11920
Four	80442	80442	26814	20111	16089	13407	11492
Five	101562	50781	33854	25391	20313	16927	14509
Six	99312	49656	33104	24828	19863	16552	14188
Seven	76860	38430	25620	19215	15372	12810	10980
Eight	90558	45279	30186	22640	18112	15093	12937
Nine	85884	42942	28628	21471	17177	14314	12270
Ten	69384	34692	23128	17346	13877	11564	9912
Yes	75348	37674	25116	18837	15070	12558	10764
No	60270	30135	20090	15068	12054	10045	8610
Hello	78240	39120	26080	19560	15648	13040	11178
Dial	100080	50040	33360	25020	20016	16680	14298
Close	82704	41352	27568	20676	16541	13784	11815
Open	93438	46719	31146	23360	18688	15573	13349
Start	87480	43740	29160	21870	17496	14580	12498
Stop	81000	40500	27000	20250	16200	13500	11572
On	67584	33792	22528	16896	13517	11264	9655
Off	77850	38925	25950	19463	15570	12975	11122

[1] Least significant bits over spoken audio samples

We have conducted 100 tests on five people with LSB-2 and an image with 965594 samples available as shown in .

TABLE 2 - USING LSB VALUE 2 ON FIVE PEOPLE

Audio Samples	Amir	Ayo	Jim	Sameh	Tope
One	40710	36762	39669	40500	42525
Two	49023	32160	40581	31758	39186
Three	41718	40680	35640	60060	41481
Four	40221	33048	41490	50508	39150
Five	50781	45444	40320	57885	48615
Six	49656	45162	46593	50220	53820
Seven	38430	46458	46704	41586	60306
Eight	45279	38700	45477	66192	60720
Nine	42942	38952	40083	48216	53169
Ten	34692	36828	34968	33165	47619
Yes	37674	51894	40704	40719	48375
No	30135	41028	35073	42303	28980
Hello	39120	43056	39480	40260	41760
Dial	50040	43758	41463	42159	48834
Close	41352	45810	51156	49590	54600
Open	46719	45024	41775	41310	41004
Start	43740	56115	49266	52923	51960
Stop	40500	50466	43446	41616	47430
On	33792	41832	37512	34398	45387
Off	38925	41880	36864	41820	48600

Results Comparison with Different People

We tested our model on samples from five people with LSB value 2. The difference of highest and lowest has been calculated to show the range of data usage in an image that has 965594 pixels available as shown in

Table 1, which gives us an average of 25392.6 of samples, needed to hide an audio sample and still have an average 71161.4 of available and unused pixels

TABLE 1 - RANGE OF PIXELS NEEDED TO HIDE ONE SPOKEN WORD

People / Value	Amir	Ayo	Jim	Sameh	Tope
Highest Value	49023	56115	51156	66192	53820
Lower Value	30135	32160	34968	31758	28980
Difference	20646	23955	16188	34434	31740

Discussion and conclusions

In this paper, we have examined the authentication process in the contexts of the e-learning classroom, virtual exam, and virtual presence. In these environments it is difficult to identify who is sitting behind the machine, raising the possibility of cheating in an assessment. Therefore, we investigated a non-intrusive authentication process that continues throughout the duration of the session and does not interrupt the educational environment. We used voice interaction that is performed by the user to interact and solve questions in the learning environment, and we embedded the voice interaction in the exam or written transcript using a concept known as steganography, which enables us to be secure and transparent at the same time.

To meet the requirements of a transparent continuous authentication process we have designed the protocol to satisfy transparency and continuous authentication by embedding voice streams into colour digital images using the least significant bits in an image, The results show that image data is fully capable of holding and encapsulating speech samples that can be used for further processing such as voice identification. When using colour photographic images and using three least significant bits the effect was visually unseen on the image, when using images containing text and using five least significant bits the effect was visually unseen, and when using seven the data was still readable. We have shown that the amount of data inserted is inversely proportional to visual detection. However, the results show that the number of samples for a speech sample is varied, and the number of samples itself should not be used as a factor in the authentication procedure and the focus should be on the content of the sample.

The result is a continuous authentication process that uses a steganography method as voice data encapsulation inside colour images that represent the exam or written transcript. The results of our experiments also show that it is possible to use other types of stream data source with any matrix data type transfer medium. Further, our method is cryptographically agnostic since any cryptographic method can be applied to our stenographic encapsulation approach.

References

Abolghasemi, M, H Aghainia, K Faez, and M A Mehrabi. 2008. “LSB Data Hiding Detection Based on Gray Level Co-Occurrence Matrix (GLCM).” In Proc. Int. Symp. Telecommunications IST 2008, 656–659.

Agulla, Elisardo González, Luis Anido Rifón, José L Alba Castro, and Carmen García Mateo. 2008. “Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments.” In ICALT ’08: Proceedings of the 2008 Eighth IEEE International Conference on Advanced Learning

Technologies, 551–553. Washington, DC, USA: IEEE Computer Society.

Apampa, K M, G B Wills, and D Argles. 2009. "Towards Security Goals in Summative E-Assessment Security." In ICITST-2009.

Artz, D. 2001. "Digital Steganography: Hiding Data Within Data." IEEE_M_IC 5 (3): 75–80.

Bingham, Lisa Blomgren. 2008. "Full Disclosure: The Perils and Promise of Transparency, by Archon Fung, Mary Graham, and David Weil, Cambridge: Cambridge University Press, 2007, 282 Pp., 28.00, Hardcover." Journal of Policy Analysis and Management 27 (1): 218–221.

Burrows, Michael, Martin Abadi, and M. Needham. 1989. "A Logic of Authentication." Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 426 (1871): 233–271.

Chan, Y.-T.F., C A Shoniregun, G A Akmayeva, and A Al-Dahoud. 2009. "Applying Semantic Web and User Behavior Analysis to Enforce the Intrusion Detection System." In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference For, 1–5.

Chang, Chin-Chen, Ju-Yuan Hsiao, and Chi-Shiang Chan. 2003. "Finding Optimal Least-Significant-Bit Substitution in Image Hiding by Dynamic Programming Strategy." Pattern Recognition 36 (7): 1583–1595.

Chou, N, R Ledesma, Y Teraguchi, D Boneh, and J C Mitchell. 2005. "Client-Side Defense Against Web-Based Identity Theft." In 11th Annual Network and Distributed System Security Symposium (NDSS'04), San Diego.

Fadhel, NF, GB Wills, and D Argles. 2011. "Transparent Authentication in E-Learning." Information Society (i-Society), …: 336–342.

Henriques, Adrian. 2007. Corporate Truth: The Limits to Transparency. Earthscan.

Johnson, N F, and S Jajodia. 1998. "Exploring Steganography: Seeing the Unseen." IEEE Computer.

Johnson, NF, and S Jajodia. 1998. "Exploring Steganography: Seeing the Unseen." IEEE Computer 31 (2): 26 – 34.

Katzenbeisser, Stephan, and Fabien Petitolas. 2000. "Information Hiding Techniques for Steganography and Digital Watermaking." EDPACS: The EDP Audit, Control, and Security Newsletter Volume 28 (October 2012): 1–2.

King, CG, RW Guyette, and C Piotrowski. 2009. "Online Exams and Cheating: An Empirical Analysis of Business Students' Views." The Journal of Educators Online 6: 1.

Kumar, Suthikshn. 2007. "Steganographic Approach to Copyright Protection of Audio." In Audio Engineering Society Convention 122.

Leite, Julio, and Claudia Cappelli. 2010. "Software Transparency." Business & Information Systems Engineering 2 (3): 127–139.

Lie, Wen-Nung, and Li Chun Chang. 1999. "Data Hiding in Images with Adaptive Numbers of Least Significant Bits Based on the Human Visual System." In Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference On, 1:286 –290 vol.1.

Lin, Chu-Hsing, Jung-Chun Liu, Chih-Hsiong Shih, and Yan-Wei Lee. 2008. "A Robust Watermark Scheme for Copyright Protection." In Proc. Int. Conf. Multimedia and Ubiquitous Engineering MUE 2008, 132–137.

Matsumiya, Kenta, Soko Aoki, Masana Murase, and Hideyuki Tokuda. 2003. "Active Authentication for Pervasive Computing Environments." Software Security—Theories : 28–41.

Robison, T, and S Tanimoto. 2007. "Controlling Transparency in an Online Learning Environment." In Proc. IEEE Symp. Visual Languages and Human-Centric Computing VL/HCC 2007, 77–80.

Rovai, Alfred. 2001. "Building Classroom Community at a Distance: A Case Study." Educational Technology Research and Development 49 (4): 33–48.

Sasse, MA, S Brostoff, and D Weirich. 2001. "Transforming the 'Weakest Link'—a Human/computer Interaction Approach to Usable and Effective Security." BT Technology Journal 19 (3): 122–131.

Sharp, Toby. 2001. "An Implementation of Key-Based Digital Signal Steganography." In Information Hiding, edited by Ira Moskowitz, 2137:13–26. Springer Berlin / Heidelberg.

Skopin, D E, I M M El-Emary, R J Rasras, and R S Diab. 2010. "Advanced Algorithms in Audio Steganography for Hiding Human Speech Signal." In Proc. 2nd Int Advanced Computer Control (ICACC) Conf, 3:29–32.

Ssemugabi, Samuel, R de Villiers, and R de Villiers. 2007. "A Comparative Study of Two Usability Evaluation Methods

Using a Web-Based e-Learning Application." Proceedings of the 2007 Annual Research: 132–142.

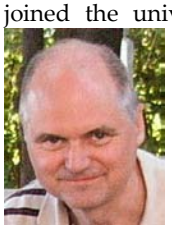
Wang, Huaiqing, and Shuozhong Wang. 2004. "Cyber Warfare: Steganography Vs. Steganalysis." Commun. ACM 47 (10) (October): 76–82.

Zamani, M, A Manaf, R B Ahmad, F Jaryani, H Taherdoost, and A M Zeki. 2009. "A Secure Audio Steganography Approach." In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference For, 1–6.

Zhi-ping, Zhou, Sun Zi-wen, Kang Hui, and Ji Zhi-Cheng. 2007. "Steganalysis for Quantization Index Module Hiding Scheme Based on Guassian Distribution." In Proc. IEEE Int. Conf. Control and Automation ICCA 2007, 1591–1593. doi:10.1109/ICCA.2007.4376628.

Zhou, Zhiping, and Maomao Hui. 2009. "Steganalysis for Markov Feature of Difference Array in DCT Domain." In Proc. Sixth Int. Conf. Fuzzy Systems and Knowledge Discovery FSKD '09, 7:581–584.

Nawfal F. Fadhel is a graduate of Baghdad College in 2001 then attended first 3 years of his academic carrier in Mansour university college till 2005 studying software engineering and then later graduate with honours from Al Ahlyaa Amman university in 2007, in 2008 he joined the university of Southampton graduating with a masters degree in software engineering and currently a postgraduate member studying for a PhD in computer Science.



David Argles has had a long and varied career, which has never strayed too far away from electronics and computing. He is primarily interested in online security, and in particular, security issues relating to eLearning. Strong authentication is one aspect of this; also the concept of "presence", the protection of personal data, and ensuring the validity of the results of online examinations taken in remote locations.

Richard M Crowder was born in Macclesfield, Cheshire, UK in 1953. He received his BSc in Engineering and PhD in Electrical Engineering from the University of Leicester in 1974 and 1977 respectively.

Following a period in Machine Tool manufacturing He joined the academic staff of the University of Southampton in 1982 and is currently a Senior Lecturer in the Agents, Interaction and Complexity Research Group, within Electronics and Computer Science. His research interests are in the application of information technology to manufacturing industry and robotics, and have published over 150 papers in this area. In addition he is the lead lecturer for a number of modules taught primarily to electrical and electromechnical engineers, as well as the Examinations Officer for Electronics and Computer Science. Dr Crowder is a member of the Institution of Engineering and Technology.

Gary B. Wills is an Associate Professor, in Computer Science at the University of Southampton. He graduated from the University of Southampton with an Honours degree in electromechanical engineering, and then a PhD in Industrial hypermedia systems. He is a Chartered Engineer and a member of the Institute of Engineering Technology. Gary is also a Principal Fellow of the Higher Educational Academy. He is also an adjunct professor at the Cape Peninsular University of Technology.

Gary's main administrative role within the school is joint programme co-ordinator for the IT in Organisation degree programme.