Transparent Authentication In E-Learning

Nawfal F Fadhel
School of Electronics and Computer Science
University of Southampton, UK
nff1g08@ecs.soton.ac.uk

Gary B Wills
Learning Societies Laboratory
University of Southampton, UK
gbw@ecs.soton.ac.uk

David Argles
Learning Societies Laboratory
University of Southampton, UK
da@ecs.soton.ac.UK

***Abstract*—In the context of on-line assessment in e-learning a problem arises is that someone taking an exam may wish to cheat by handing over personal credentials to someone to take their place in an exam. This differs from authenticating for on-line banking where it is in the user interest to ensure safe and correct authentication. Our proposed solution is to digitally sign the student work by embedding voice samples in the exam paper at regular intervals. In this investigation we have demonstrated that transparent steganography can provide an effective mechanism for achieving such a good goal.**

***Index Terms*—Transparency, Authentication, E-learning, Steganography**

I. 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 can not identify who is sitting on the other end [2]. It's true we have the concept of classical authentication to prove a claim of identity [5]. A concept which is designed to protect a persons identity; this concept is mature and well developed in information technology today. However this situation is reversed in e-learning situation, the authentication process which was deigned to protect personal identity; the user will sometimes be willing to exploit the protocol for the purpose of cheating, making himself an accomplice by falsifying information or giving information to a person who will help them to pass an on-line exams. In Apampa et al. [3] work has demonstrated a solution for the previous statement 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 mentioned *"manual authentication"* she is actually referring to the physical process of ongoing invigilation, rather that the initial process of authentication. The current monitoring solutions are based on mutual trust among individuals like trust between student and invigilators.

We believe this procedure places a burden on the authentication process because the only way we can validate the authentication is through people who are considered the weakest link in computer security. We can overcome some issues in human behavior, but not all [12, 6].

There are more than a few proposed solutions to the continuous authentication problem. Previous solutions introduced mild to heavy authentication processes (a presence)and are not entirely user friendly because of their intrusive behavior, for example scanning your finger print every 5 minutes or sitting still for the biometric to be taken [2]. The weight of the authentication process sometimes causes an intimidating atmosphere which affects the morale of the exam participant, or introduce a hesitant participation in an e-lecture or remote brain storming session through web seminars.

We aim to design a non-intrusive authentication protocol , That confirms presence 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 electronic learning providers to act transparently towards the general public. For example if we secure an exam transcript electronically, we are required to make an available copy of the document if requested, and that is transparency according to[**?** 10].

Finally we have chosen steganography to use as a secure data encapsulation for data transfer. so we proposed 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 steganographic encapsulation.

II. E-Learning

E-learning is an abbreviation for electronic learning. A new concept that uses 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. For the purpose of this paper we explain the nature of e-learning environment and material variation.

A. E-Learning and E-Assessment

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. Therefore e-assessment is an assessment process of a taught course regardless whether the teaching method was on-line or in class teaching. In table 1 is a

Nawfal F Fadhel is with the Department of Engineering, Science and Mathematics, School of Electronics and Computer Science, Southampton, United kingdom, e-mail: nff1g08@ecs.soton.ac.uk.

Table I
ASSESSMENT AND TEACHING ACRONYMS

Assessment	Learning
Computer based test(CBT)	Computer based learning(CBL)
Internet based test(IBT)	Internet based learning(IBL)
Web based test(WBT)	Web based learning(WBL)

categorization of electronic approaches to learning and testing procedures.

After categorizing the educational material now we illustrate the content in the next section.

B. E-learning material Variations

The nature of the educational material is varied and depends on the academic teaching methods and scientific content, we will summarize the variation to two sections, the exam based material and the learning based material. 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 in the topic of this paper is the authentication process in the 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.

Table II
EDUCATIONAL MATERIAL VARIATION

Exam based material	Learning based material
Multiple choice questions	Power point presentation
Essay questions	Video presentation
Lab questions	Webinar Session

III. SHORTCOMINGS IN E-LEARNING AND E-TESTING

When we think of e-learning or on-line-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 centers (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.

1) Misplaced trust in individuals, such that the students are trying to cheat and invigilators being too lenient and sympathetic to students which has negative a impact on exam results [8].
2) A great weight of the authentication procedures are manual and not computerized and this not only affects the authentication process but also cripples anonymity[8].
3) Lack of friendliness in the exam environment due to the invigilator's presence or the burden imposed by the authentication procedure [2].
4) Shyness of people in lectures when their identity is exposed which results in lessened participation [2].

We know that these points are valid for today's approaches to e-learning [2, 8, 11] 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.

IV. 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 point of view, whether it was a user target, organization or a social group [10]. 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 foundation for the design will target the right the solutions to the authentication process in e-learning.

A. Transparency in education

Organizational transparency 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. Student 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 to students, while other studies have produced results that state when students are given freedom and more space they will be more productive.

B. Transparency and Academic integrity

According to Bingham [4] "*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 transparency context. The disclosure of secure information must have two sides, first we need to ensure that we can authenticate the information and it's source so we can remedy disinformation, and by disinformation we mean falsification of information or stealing copyrighted material and posing as the originating source. Second side is 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 insure 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.

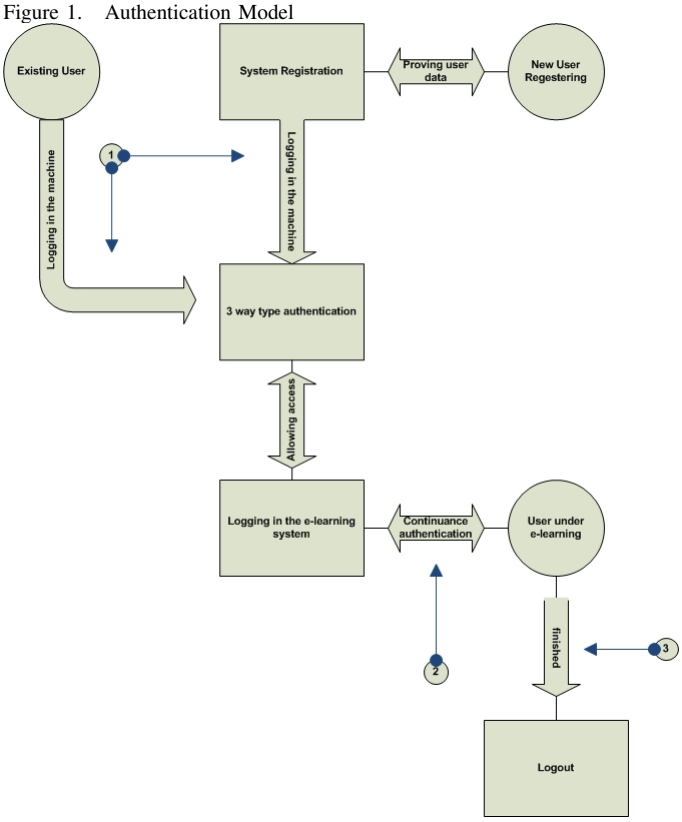
V. TRANSPARENT AUTHENTICATION

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 which encapsulates your information and forms identifiable attributes of a person or an object within the system.

Transparent Authentication as explained in section 4.2 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.

Figure 1. Authentication Model



A. Authentication in continuous presence

Due to the demand of the e-learning education process, the user is required to be continuously present [3] behind the computer when talking exams on-line. We needed to formulate a process protocol for continuous authentication as illustrated in figure 1 in step two. Previous attempts to solve this problem placed a heavy burden on users because of the frequency demand of authentication. We believe our model will achieve that goal efficiently because the use of non-intrusive authentication procedures will make our model will feel transparent to the user by reducing the needed effort to authenticate. This process will produce an incentive for the user to interact with electronic system since it's a lightweight authentication protocol.

B. Authentication in identity proofing

Personal authentication is established by providing the appropriate credentials to prove that you are who you claim to be. This point is illustrated in the figure 1 in step one. 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. We will not go into inter-working of this protocol because it's not within our scope of research and has been discussed in many studies such as [5].

VI. STEGANOGRAPHY

"*Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means covered writing. It includes a vast array of secret communications methods that conceal the messages very existence*" [7].

This is the most common definition for steganography that is mostly used in textbooks and research papers. As it states in the second paragraph the existence of 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 messageZhou and Hui [16], Abolghasemi et al. [1], Zhi-ping et al. [15] .

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 the fact is in 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 can not 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 there exist a hidden message is a must in insuring transparency we need to modify the current steganography not to 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: is a process of adding or embedding information into a digital media to prove its origin and protect the intellectual property.
- Digital Signature Authentication: Digital signature holds the same value of a hand signature but is constructed using digital means to render it immune to counterfeiting.
- Digital Signature is used in signing confidential document and is an undeniable by the originator and receiver of the message.
- Digital Linkage and Storage: 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.

A. Modern steganography

Modern steganography is a step further than classical steganography and a redefined model is required. We integrate the use of cryptographic keys to achieve security then use data encryption into steganography to prevent cryptanalysis, and

that in itself 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 are previous works done by Sharp [13] which propose 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 steganographic procedure acts as a encapsulation to the hidden data and this encapsulated data is secured by a cryptographic key. Second, we added encryption to steganography by manipulating the hidden data, not the cover medium in the data preparation step this act as a counter measure to steganographic detection [16, 1, 15]

B. Secure steganography

We will now take 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, the key is a main component in retrieving the secure data from the digital storage. This statement is still ambiguous till this point and needs a further explanation. First, we have two components. The cover medium which will serve as a storage medium and 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.

C. Encrypted steganography

This is a simple question of why do we need to encrypt an existing security protocol and the reason is simple. Because of the advanced method mentioned in [16, 1, 15] it is relatively easy to detect data manipulation. Since it's relatively easy to detect then it's relatively easy to extract the hidden information [14]. 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 [16, 1, 15] to detect changes in digital media and indicate the usage of stenographic techniques that malicious attackers, we think it's a good idea to incorporate the encryption into our scheme of steganography to prevent cryptanalysis. Because even if the malicious attackers found out that the media contains hidden data (audio medium stream) and they where able to extract the data they can not obtain its contents without the key which contains the encryption sequence.

VII. Transparency, steganography and Authentication

The reason we invented the concept of modern steganography is to cope with electronic education as it will be explained in the next section. In order to use electronic education we need a new encapsulation that is able to carry both data and security protocols.

Now the big question is how do we fit transparency, steganography and authentication into one model. The answer is simple, 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 institutes alike. The user will be notified a head of a class or exam that voice identification will be used by authentication and the voice interaction will serve in authenticating the student and answering questions.

A. Benefits of Transparent Authentication

According to Rovai [11] they theorized that there are four component to a class room community. Spirit, Learning, Interactions and Trust. We agree with Rovai and Lucking's principles and believe that if these conditions are accommodated in the E-learning design, we can achieve a superior learning experience.

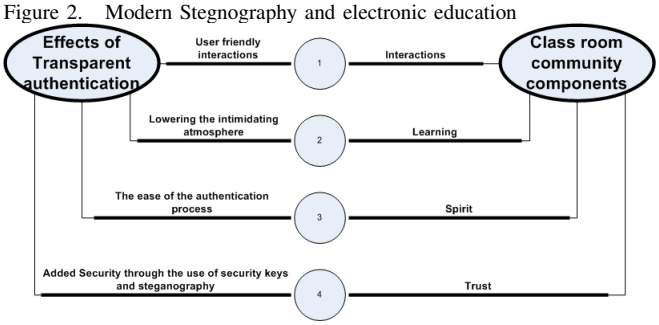
1. The ease of the authentication process With Spirit : Spirit is the feeling belonging, acceptance and recognition. these feeling are considered somewhat fragile and easily affected, if we bombard the process with heavy authentication it will break The spirit component in the classroom community.

2. 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.

3. 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.

4. 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.

Figure 2. Modern Stegnography and electronic education



The fact is our four legged model of steganography fits perfectly with values of e-learning [11] as illustrated in figure 2.

VIII. Transparent Authentication Protocol

The result of our efforts to solve the short comings in e-learning has resulted in the construction of transparent authen-

tication protocol. Using the concept of continuous authentication in transparency frame work within the area of e-learning and achieving it through redefining steganographic techniques and constructing a new protocol filling the requirements and specification of e-learning model.

The transparent authentication protocol functions as a continuous presence authenticator using voice identification through interactions between the user and the electronic system then encapsulating the data to comply with 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 institutes alike. The user will be notified a head of a class or exam that voice identification will be used by authentication and the voice interaction will serve in authenticating the student and answering questions.

Figure 3. Encoding Process

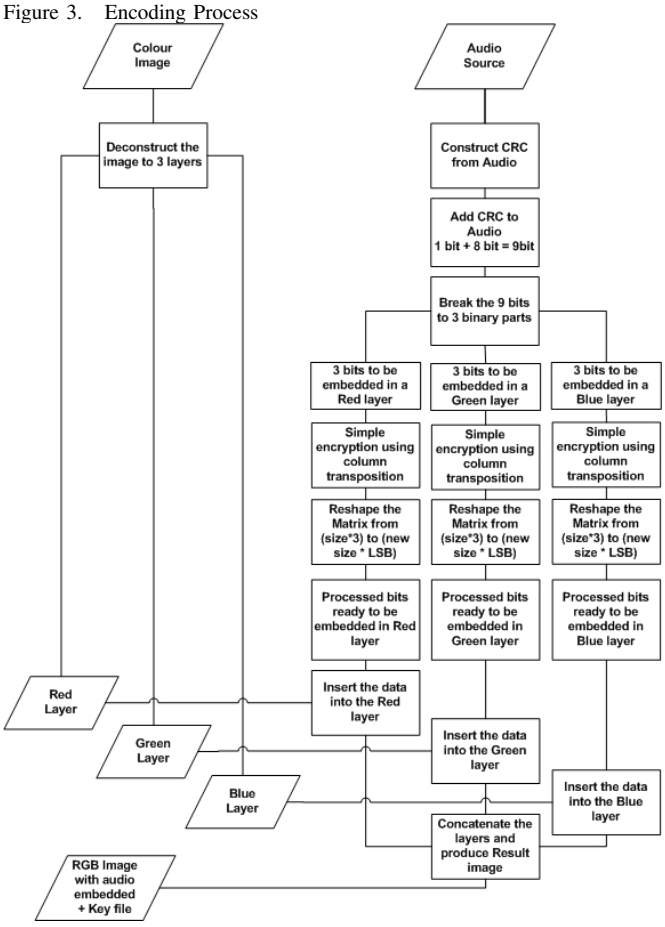


Figure 3 describes the data encapsulation phase in which the voice data is embedded in image cover medium. Encoding process requires prepossessing on voice and image data, in which the image data is deconstructed into red, green, blue layers. Voice data is merged with cyclic redundancy check and then segmented into three data sets.

The data set can be customized to the desired bit size ranging from (1 .. 7) , then the data set will be embedded into an image layer occupying the least significant bits in an image layer i.e red.

Figure 4. Bit Replacement

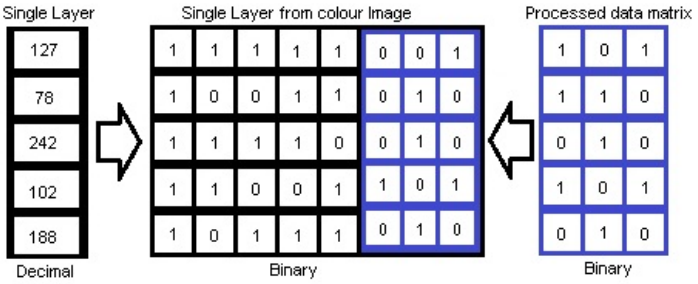


Figure 4 is an example of bit replacement on binary-decimal data, where we are using the 3 least significant bits of the image and replacing them with the processed data set with the same size. The results of the quality of the encoding process depends on the number of least significant bits used.

A. Our Results in Summary

We will go through our Results achieved on pursuing transparent authentication in e-learning. As we have achieved all our goals that we set-out to begin with. Explored new areas of e-learning and touched upon others areas that where often over-looked. We also tested with wide range of inputs and our results showed that they can be used in other areas of security,data storage and e-learning. In summary they are as follows :

1) We diagnosed the current e-learning process and identified that it's lacking or has a problem in proving continuous presence.
2) We noted that student monitoring procedures should not be intrusive.
3) We identified that voice matching is sufficient and there is no need spend processing power and time to do voice recognition.
4) We explored the capacity of images to hold steganographic voice data.
5) We enhanced security procedures by putting two security concepts together, data security and encryption.

IX. Conclusions

In this paper we combined two security concepts, authentication procedures and modern steganography under a transparent framework. We explained how classical authentication procedures differs from continuous authentication [3]. Modern steganography is not a new concept but our implementation that included encryption and key cryptography is new. All that was achieved in the name of transparency. The result was a transparent authentication model.

We have concluded from our results that a secure encrypted steganography is achievable. We have demonstrated how it can be used in e-learning as a part of the authentication procedure. We have proved that it could have other uses in security and e-learning. We see that the usage of a light-weight authentication protocol will have a positive effect on the classroom community in e-learning.

We also believe our work will be beneficial in the area of e-learning and bring about more acceptance of e-learning by the general audience by simplifying security procedures.

X. Future Work

Our research have opened other areas where further studies could be preformed and results perfected. With this intention in mind we outlined future work possibilities to be conducted and they are as follows :

1) We believe our work will further progress in the e-learning model.
2) Our encryption model is still a proof of concept and easily decipherable. We hope to devise a more sophisticated scheme.
3) Construct guidelines to build a user-friendly interface that includes voice interactions within its design.
4) Include image acquisition sources like web-cameras, video-cameras and image scanners in our data sources for the cover medium.
5) Consider other sources or types of data streams as hidden data to used in encoding.

By following these outlines we expect to achieve three goals. First, the construction of a user friendly authentication process for proving availability in an e-learning environment. Second, accounting for availability and proving participation in work or class and as a result copyrighting ideas and data rights management [9]. And lastly, achieving data security through hiding Speech data or other streams within colour images which is referred to as steganography.

References

[1] M. Abolghasemi, H. Aghainia, K. Faez, and M. A. Mehrabi. Lsb data hiding detection based on gray level co-occurrence matrix (glcm). In *Proc. Int. Symp. Telecommunications IST 2008*, pages 656–659, 2008. doi: 10.1109/ISTEL.2008.4651382.

[2] Elisardo González Agulla, Luis Anido Rifón, José L. Alba Castro, and Carmen García Mateo. 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*, pages 551–553, Washington, DC, USA, 2008. IEEE Computer Society. ISBN 978-0-7695-3167-0. doi: http://dx.doi.org/10.1109/ICALT.2008.184.

[3] K.M Apampa, G.B Wills, and D Argles. Towards security goals in summative e-assessment security. In *ICITST-2009*, November 2009. URL http://eprints.ecs.soton.ac.uk/18487/.

[4] Lisa Blomgren Bingham. 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, 2008. URL http://econpapers.repec.org/RePEc:wly:jpamgt:v:27:y:2008:i:1:p:218-221.

[5] Michael Burrows, Martín Abadi, and Roger Needham. A logic of authentication. *ACM TRANSACTIONS ON COMPUTER SYSTEMS*, 8:18–36, 1990.

[6] Y.-T.F. Chan, C.A. Shoniregun, G.A. Akmayeva, and A. Al-Dahoud. 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*, pages 1 –5, 2009.

[7] N. F. Johnson and S. Jajodia. Exploring steganography: Seeing the unseen. *Computer*, 31(2):26–34, 1998. doi: 10.1109/MC.1998.4655281.

[8] King. Online exams and cheating: An empirical analysis of business studentsŠ views. *Journal of Educators Online*, 6:1, 2009.

[9] Chu-Hsing Lin, Jung-Chun Liu, Chih-Hsiong Shih, and Yan-Wei Lee. A robust watermark scheme for copyright protection. In *Proc. Int. Conf. Multimedia and Ubiquitous Engineering MUE 2008*, pages 132–137, 2008. doi: 10.1109/MUE.2008.17.

[10] T. Robison and S. Tanimoto. Controlling transparency in an online learning environment. In *Proc. IEEE Symp. Visual Languages and Human-Centric Computing VL/HCC 2007*, pages 77–80, 2007. doi: 10.1109/VLHCC.2007.36.

[11] Alfred Rovai. Building classroom community at a distance: A case study. *Educational Technology Research and Development*, 49:33–48, 2001. ISSN 1042-1629. URL http://dx.doi.org/10.1007/BF02504946. 10.1007/BF02504946.

[12] M A Sasse, S Brostoff, and D Weirich. Transforming the Śweakest linkŠ Ů a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19:122–131, 2001. ISSN 1358-3948. URL http://dx.doi.org/10.1023/A:1011902718709. 10.1023/A:1011902718709.

[13] Toby Sharp. An implementation of key-based digital signal steganography. In Ira Moskowitz, editor, *Information Hiding*, volume 2137 of *Lecture Notes in Computer Science*, pages 13–26. Springer Berlin / Heidelberg, 2001. URL http://dx.doi.org/10.1007/3-540-45496-9_2. 10.1007/3-540-45496-9-2.

[14] M. Zamani, A. Manaf, R.B. Ahmad, F. Jaryani, H. Taherdoost, and A.M. Zeki. A secure audio steganography approach. In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, pages 1 –6, 2009.

[15] Zhou Zhi-ping, Sun Zi-wen, Kang Hui, and Ji Zhi-Cheng. Steganalysis for quantization index module hiding scheme based on guassian distribution. In *Proc. IEEE Int. Conf. Control and Automation ICCA 2007*, pages 1591–1593, 2007. doi: 10.1109/ICCA.2007.4376628.

[16] Zhiping Zhou and Maomao Hui. Steganalysis for markov feature of difference array in dct domain. In *Proc. Sixth Int. Conf. Fuzzy Systems and Knowledge Discovery FSKD '09*, volume 7, pages 581–584, 2009. doi: 10.1109/FSKD.2009.230.