2014

Securing identity information with image watermarks

Brian Cusack
Auckland University of Technology, brian.cusack@aut.ac.nz

Reza Khaleghparas
Auckland University of Technology, reza.khaleghparast@aut.ac.nz

Originally published in the Proceedings of the 12th Australian Information Security Management Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/164

SECURING IDENTITY INFORMATION WITH IMAGE WATERMARKS

Brian Cusack, Reza Khaleghparast
Auckland University of Technology, Auckland, New Zealand
brian.cusack@aut.ac.nz   reza.khaleghparast@aut.ac.nz

Abstract

In this paper, we describe the requirements for embedding watermarks in images used for identity verification and demonstrate a proof of concept in security sciences. The watermarking application is designed for verifying the rightful ownership of a driving license or similar identity object. The tool we built and tested embeds and extracts watermarks that contain verification information of the rightful owner. We used the human finger print of the rightful owner as the watermark. Such information protection mechanisms add an extra layer of security to the information system and improve verification of identification attributes by providing strong security. The issues of usability and cost are also discussed in the context of the social acceptability of access controls.

Keywords
Security, Images, Watermarks, Verification, Design, Usability

INTRODUCTION

Three authentication attributes are required to verify the rightful ownership of an identity card. These cards are widely used for access control of human participation in motor vehicle driving, liquor access, library and other memberships. The extent to which attribution is required is often decided by the risk to be mitigated or by the usability function (Oligeri, Chessa, Di Pietro, and Gianta, 2011). Risk for motor vehicle drivers is usually more highly prioritized than gym membership and often attribution for verification is proportional to the risk register. Usability, however often acts as a moderating variable so that if an attribution activity such as retina scanning or full fingerprinting is time consuming or socially unacceptable then a lesser or better fitting option is adopted. (Usability is used throughout this paper to address the human expectations for seamless technology use.) Usability often determines that a card has a photograph, a signature and a third person referral contact; to which the verification agent can make visual recognition and or seek further verification by cross referencing from the other attributions such as requesting a signature, a phone number or contacting a third party. These measures have cost effective control but are open for improvement and tampering (Nukamura, Katayama, Yamamuro, and Sonehara, 2004).

The more general use of biometric attributes is enhancing the quality of verification but not always satisfying usability requirements (Sherekar, Thakare, and Jain, 2008). Our proposal is to demonstrate a tool that embeds the finger print of the rightful owner of a card in the photographic image. Many laptops and mobile devices these days have finger print scanning inputs that only require a user to run the index finger over a small scanner or a screen print cell (O'Ruanaidh, Dowling, and Boland, 1996). The proposition is that an identity card embedded with our watermark can also be run across the same canner and the two impressions compared with software that usually comes free of charge with the operating system. A verification agent would then have two attributes present (Blanton, Zhang, and Frikken, 2013). Both are quick and easy to process and one presents strong security. In such a situation a third authentication attribute may not be necessary and the usability of the security mechanism enhanced (Sherekar, Thakare, Jain, Ashwini, Tijare, Deshpande, 2011).

In this paper we describe the attributes of watermarks and the tool we built for embedding fingerprints into images. The discussion addresses the risk trade-off between strong security and usability. We conclude that watermarking accompanied by readily available input surfaces and software is a working solution for identity authentication and verification processes.

WATERMARKS

A digital watermark can be either visible or invisible and is used to protect from copyright and ownership infringement. Each selected watermark requires the property of “robustness” where it is resilient to actual and potential attacks that may destroy the recognition or retrieval of the watermark (Cayre, Fontaine, and Furon, 2005). The aim of watermarking is to introduce small patterns in the target data without changing the original source. Consequently if there is illegal use of the property the owner can verify ownership of the data (Chroni, and Nikolopoulos, 2010; Johnson, Duric, Jajodia, and Memon, 2001). The use of a visible or an invisible watermark (or a combination of both) would satisfy the requirement for protection in an identity card and also the usability function for speed and utility (Liu, Ma, Zhang, Li, and Chen, 2011). The scope of watermarking security research can be established by dividing the potential field into its properties and attributes. In figure 1 the properties are listed as Media; Perceptibility; Robustness; Type; Processing Method; and, Extraction Key. These properties span the scope of watermark technologies and specify the choices that must be made for implementation (Chuhong, Kundur, and Kwong, 2006). Each property has few or many attributes that must be selected for a particular characteristic of watermark for a particular purpose or environment (Zhu, Wei, Xiao, and Wang, 2009).

.

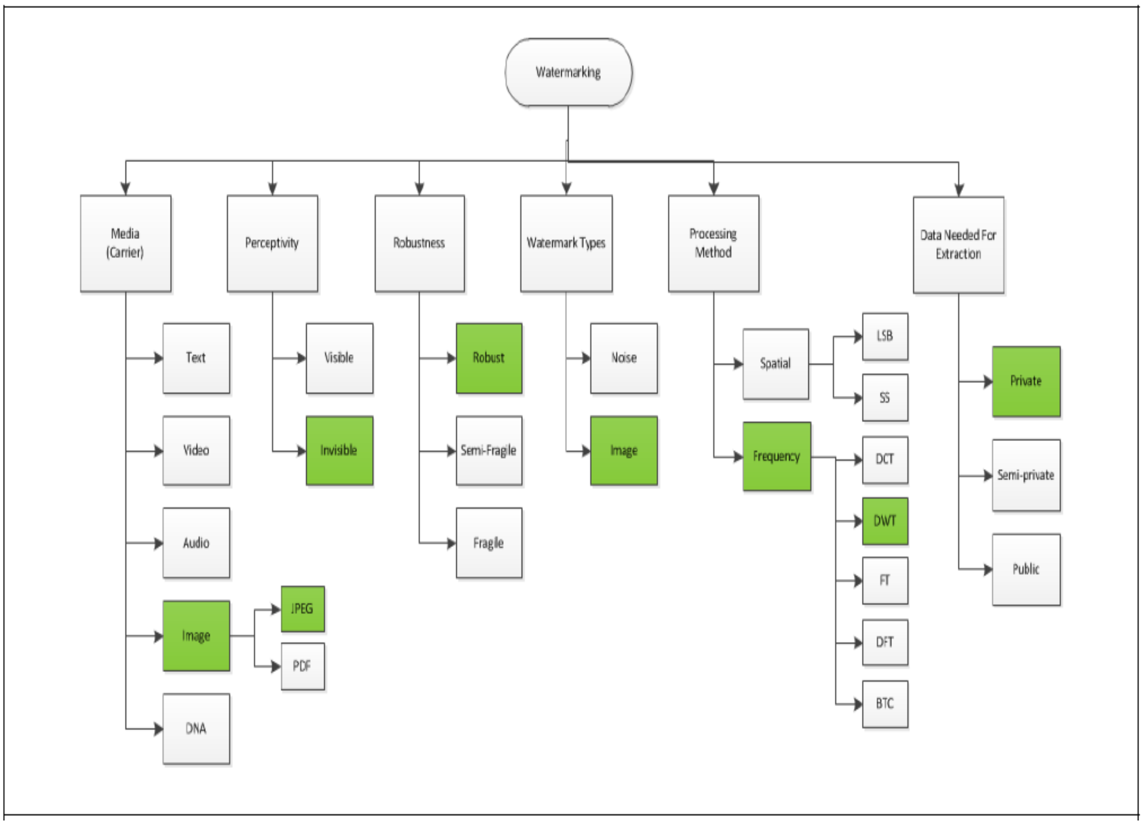


Figure 1. The Scope of Watermark Research

.

TOOL BUILD

The objective of our tool build was to scan and insert a human finger print into an image. The .bmp file was assessed an easy format to work with for testing. The test image was chosen randomly from .bmp files freely available on the web and then the tool applied. We also provided an extraction algorithm for use when a verifying agent required a comparison of a biometric scan and the embedded watermark. The Embedding details (see figure 4) show innovation in the exploitation of the three color channels (rather than the usual grey scales) and the least significant bits being applied to two bits (pixels) instead of the usual one for embedding the bit stream for the watermark.

The Embedding Algorithm

The embedding algorithm (figure 2) relies on the parallel processes of converting the cover image and the fingerprint scan into byte arrays. The arrays are computed for size. If a byte array is too large to fit inside the cover object then the scan is rejected and the process stops to be started again until size compatibility is satisfied. If the size constraint is satisfied then the array can be converted directly into bits for the grey scales or the array can be converted to exploit the color channels. Once the size and type of array are stabilized the algorithm then requires the embedding of the bit streams in the cover object. The embedding process is checked for completeness and the insertion of the fingerprint bit by bit is finalized.

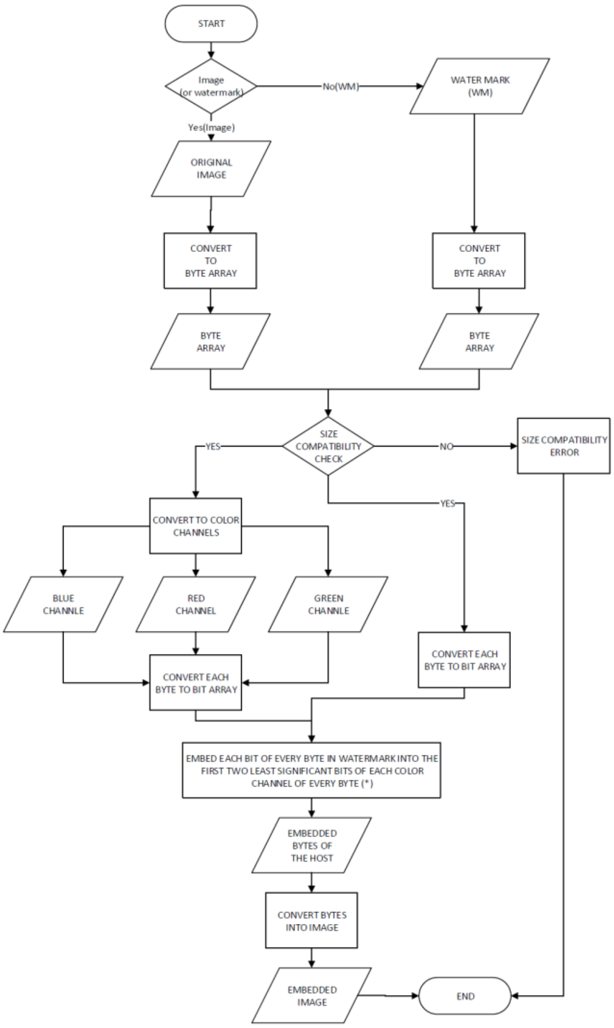


Figure 2. The Embedding Flow Chart

The Extraction Algorithm

To extract the embedded watermark the tool was designed for multiple scan interfaces. The design considered the use of such embedding for multiple instances for identity card reading and of different types of systems. Hence a public key was made available in the tool that could be invoked at any instance of scanning request. Once the watermark information was read it was then checked for tampering that may have occurred through card use or damages and the extent of tampering measured against the PSNR scales to determine if the watermark was still usable. In the case the watermark had been damaged in some ways but the PSNR was above 30% then the untampered parts could be extracted for use. If no tampering or damage had occurred then the extracted watermark could be compared with a biometric scan from the present rightful owner and authentication verified.

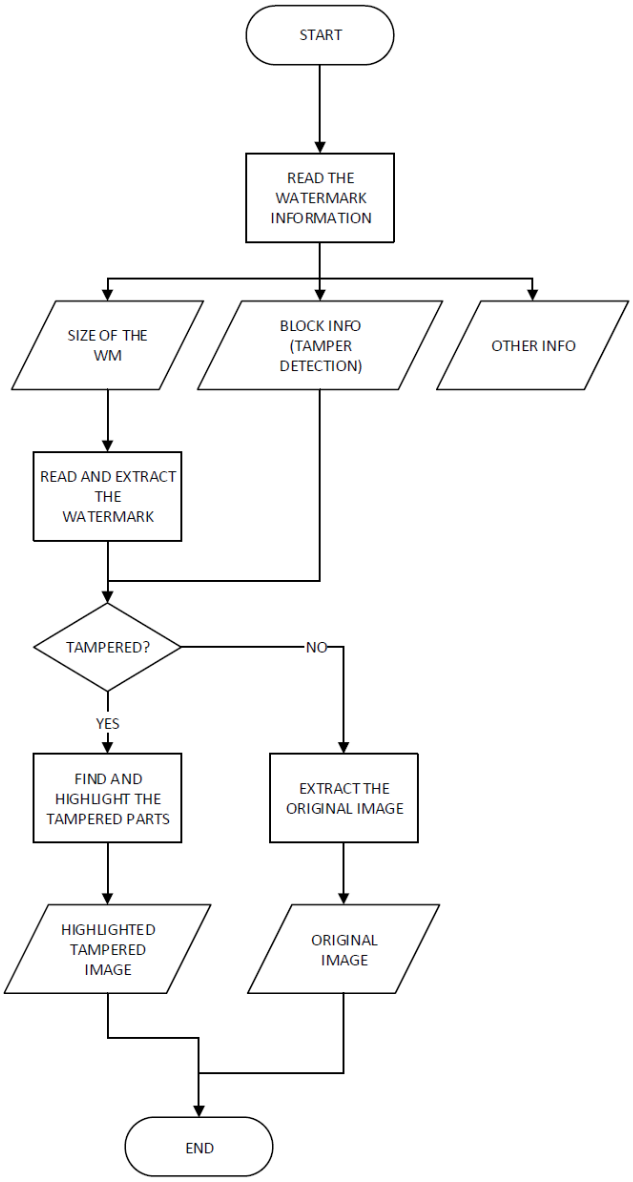

START
READ THE WATERMARK INFORMATION
SIZE OF THE WM
BLOCK INFO (TAMPER DETECTION)
OTHER INFO
READ AND EXTRACT THE WATERMARK
TAMPERED?
NO
YES
FIND AND HIGHLIGHT THE TAMPERED PARTS
EXTRACT THE ORIGINAL IMAGE
HIGHLIGHTED TAMPERED IMAGE
ORIGINAL IMAGE
END

Figure 3. The Extraction Flow Diagram

The Embedding Detail

The embedding detail is explained in figure 4 and relates to the (*) indicated in the figure 2 middle statement box. The watermark is embedded in the first 100 bytes of the image with a preference for the blue color channel as being more stable. Consequently the size check in figure 2 is critical. The watermark is broken up into eight bit bytes and inserted into the image cover object bit by bit starting with bit 0 inserting to blue, bit 1 to red, bit 2 to green and then repeated until the full bit stream representing the fingerprint is embedded. The prior determination of size assures complete embedding and no loss.

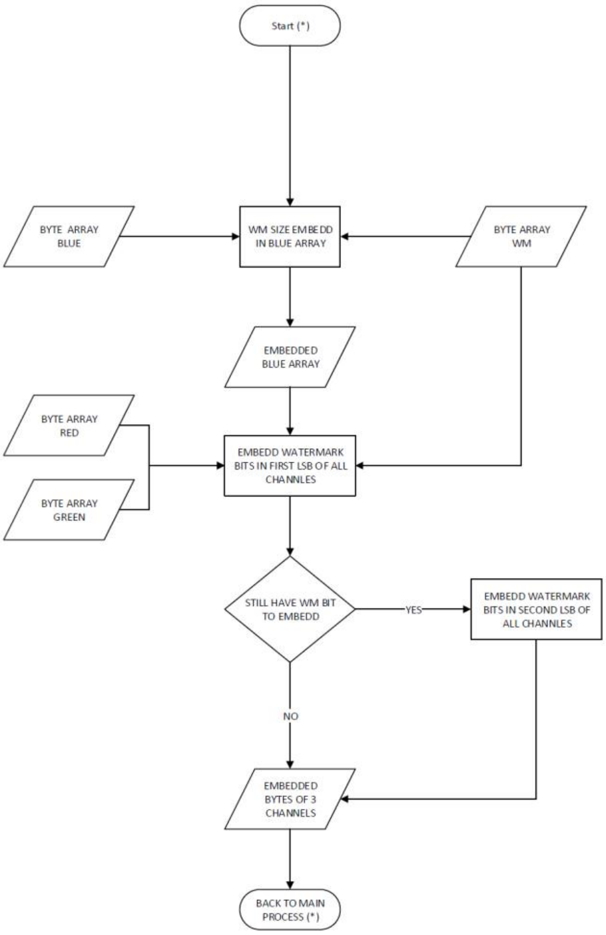
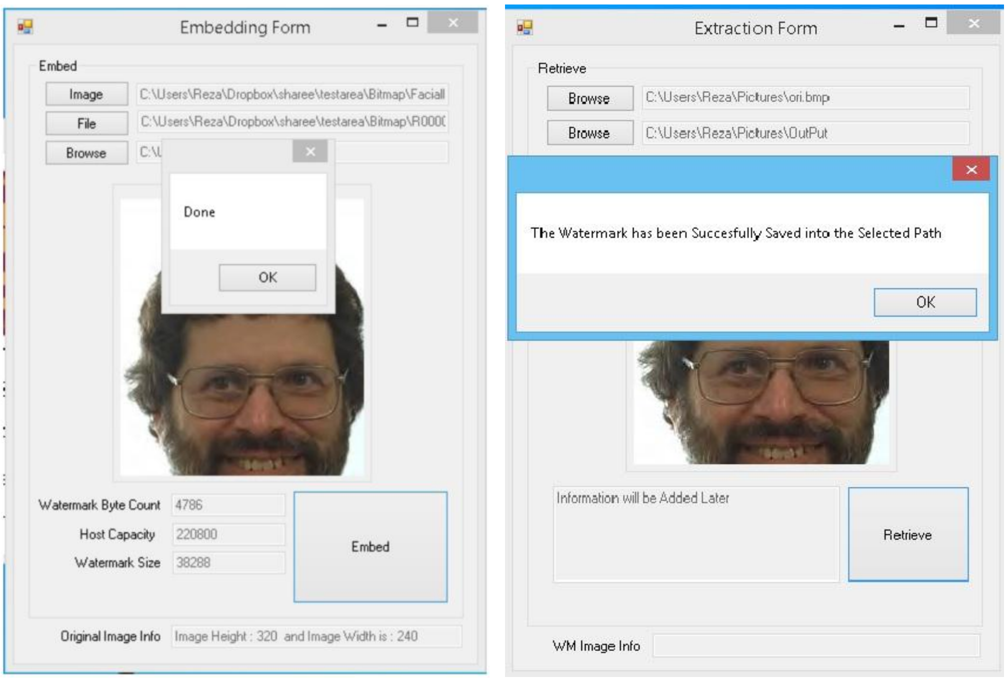

Start (*)
BYTE ARRAY BLUE
WM SIZE EMBEDD IN BLUE ARRAY
BYTE ARRAY WM
EMBEDDED BLUE ARRAY
BYTE ARRAY RED
BYTE ARRAY GREEN
EMBEDD WATERMARK BITS IN FIRST LSB OF ALL CHANNLES
STILL HAVE WM BIT TO EMBEDD
YES
EMBEDD WATERMARK BITS IN SECOND LSB OF ALL CHANNLES
NO
EMBEDDED BYTES OF 3 CHANNELS
BACK TO MAIN PROCESS (*)

Figure 4. The embedding Details

RESULTS

The results are shown in the tool forms that report the step-by-step progress through the embedding and extraction algorithms. Figure 5 reports the successful embedding of the identity card owner fingerprint into the photographic image. The embedding process was digital but the extraction can be digital or optical depending on the scan equipment available for use. The image is transferred to an identity card that may be in plastic or paper forms. The result can then be carried by the card owner and presented for verification. All watermarks have been stored digitally in the pictures themselves; therefore they can be retrieved by the same system and methodology or optical systems for authentication purposes. Figure 5 is one example of the multiple forms that present the process steps toward the completion. Testing of the research output in a simple scanner on a laptop and on a smart phone showed the test subject could be identified by the authentication attributes on and embedded in the identity card. In all instances the test subject scanned the index finger on the input devices available on the computers and then submitted the biometric scan and the watermark scan to the software on the operating systems for finger print comparison processing. Twenty different subjects were tested and in all instances the match was made and the rightful owner identified (The PSNR >30% was used for fidelity and robustness measures as mentioned above). Such results appear elementary but we are also showing that by using readily available technologies these valuable security processes can be successfully completed. The time to complete the two scans and the comparison verification took under 20 seconds. Consequently such application can be socially unobtrusive and easily fitted within usability guidelines for user satisfaction. The added strength fingerprints embed as watermarks greatly enhances the value of an identity card and the acceptability for identification.



Embedding Form

Embed

Image: C:\Users\Reza\Dropbox\sharee\testarea\Bitmap\Faciall

File: C:\Users\Reza\Dropbox\sharee\testarea\Bitmap\R000(

Browse: C:\U

Done

Watermark Byte Count: 4786

Host Capacity: 220800

Watermark Size: 38288

Original Image Info: Image Height : 320 and Image Width is : 240

Extraction Form

Retrieve

Browse: C:\Users\Reza\Pictures\ori.bmp

Browse: C:\Users\Reza\Pictures\OutPut

The Watermark has been Succesfully Saved into the Selected Path

Information will be Added Later

WM Image Info

Figure 5. Tool Form Output

DISCUSSION

Security access controls present barriers to human actions and in particular participation in benefits such as motor vehicle driving, alcohol consumption and many other recreation and social activities. Theoretically many biological and logical access controls are possible and the research of many scientists has shown that the integration of technologies with the abstractions of security science can deliver controls for human behaviors. In general, however, less is written about the impact of these security technologies on beneficial human behavior. For example in most jurisdictions the control of alcohol consumption by age requirements and disposition acts as a moderating influence for acceptable social behaviors and conduct. The critical turning point is the successful execution of the control. If the access is granted on a false positive then the potential for anti-social human behavior is high or if the access is rejected on a false negative then the system itself comes under scrutiny and it may be causal in a range of anti-social behaviors. Such thinking is often absent from the purely technical quick fix solutions to security issues. We have attempted to show by design that theory can be transferred into practice in ways that a full 360 degree appraisal of human behavior is made in conjunction with the security theory. Beneficial human behaviors may be achieved by setting the initial barrier to action (security control) in such a way that both the positive and negative attributes of risk are managed towards the required human behavior. Enhancing the correct verification of alcohol consumers with the type of security features we describe has a deliverable impact on the consequences of access control. Accurate verification has the advantage of assuring the greatest number of beneficial behaviors are achieved and the integrity of the security system is maintained.

The social acceptability of access controls is an unwritten tradeoff between the perceived cost of compliance and the benefits of non-compliance. The identity card for driving a motor vehicle for example is of high value to the user and gives access to responsible and beneficial actions. The acceptable performance of human behavior while in the authorized control of a motor vehicle demonstrates compliance with the expectations for holding the card. However the same human may calculate the financial cost of renewing a driver’s license and choose not to renew but pay the consequences. They may choose to ignore the terms and conditions of the license or have an appetite for risk that negates the purpose of authorizing access to vehicle use. In each instance the threshold for compliance has a social dimension trade-off that most drivers are prepared to calculate and then decide the tipping point. An identity card that gives access to a sports club or a bar may not be held in the same regard and have the same threshold for compliance as a motor vehicle. A human user may resist the same level of training and testing required of a driver’s license when they are 60 years of age and wish to purchase alcohol. Consequently the usability of an identity card is a trade-off that is socially calculated at every use. In our development of the tool we considered the thresholds users may have for compliance. The scanning of eyes for biometrics was considered at a higher social threshold than the scanning of one fingerprint. Similarly we calculated the cost to a service supplier of the access control. Excessively expensive equipment will only be used under duress and the equipment must be fast, accurate and efficient. Cost has many dimensions and each must be assessed for the successful implementation of security mechanisms. The availability and the technical feasibility of a security mechanism may not deliver better security unless the human and social consequences of the capability are also factored into the solution.

CONCLUSION

We have demonstrated the proof of concept that identity card security can be enhanced using software and hardware that is readily available. The level of detail presented has focused on the design and design attributes so the feasibility of the model is apparent and not lost with excessive testing output tables. The tool developed indicates that simplicity in design and attention to the building blocks of images allows a working solution to be tested. The key points in usability of speed and social acceptability have been addressed. The development of a fully standardized commercial solution would allow identity verification to proceed in a non-intrusive and time effective manner.

REFERENCES

Blanton, M., Zhang, Y., and Frikken, K. (2013). Secure and verifiable outsourcing of large-scale biometric computer computations. *ACM Trans. Info & Sys Security*, 16, 3 (TISSEC).

Cayre, F., Fontaine, C., and Furon, T. (2005). Watermarking security: theory and practice. In: *Signal Processing, IEEE Transactions on.* 53(10), 3976-3987.

Chroni, M. and Nikolopoulos, S. (2010). Encoding watermark integers as self-iniating permutations. In *Proceedings of the 3rd International Conference on Computer Systems and Technology.*

Chuhong, F., Kundur, D., and Kwong, R. H. (2006). Analysis and design of secure watermark-based authentication systems. In: *Information Forensics and Security, IEEE Transactions on.* 1(1), 43-55.

Johnson, N. F., Duric, Z., Jajodia, S., and Memon, N. (2001). Information Hiding: Steganography and Watermarking—Attacks and Countermeasures. *Journal of Electronic Imaging.* 10, 825.

Liu, Y.-C., Ma, Y.-T., Zhang, H.-S., Li, D.-Y., and Chen, G.-S. (2011). A method for trust management in Cloud computing: Data coloring by Cloud watermarking. *International Journal of Automation and Computing.* 8(3), 280-285.

Nukamura, N., Katayama, A.,Yamamuro, M., and Sonehara, N. (2004). Fast watermarking detection scheme for camera equipped cellular phone. (MUM’04).

Oligeri, G., Chessa, S., Di Pietro, R., and Gianta, G. (2011). Robust and efficient authentication of video stream broadcasting. *ACM Trans. Info & Sys Security*, 14, 1 (TISSEC).

O'Ruanaidh, J. J. K., Dowling, W. J., and Boland, F. M. (1996). Watermarking digital images for copyright protection. *Vision, Image and Signal Processing, IEEE Proceedings -.* 143(4), 250-256.

Sherekar, S., Thakare, V., and Jain, S. (2008). Role of Digital Watermark in e-governance and e-commerce. *International Journal of Computer Science and Network Security.* 8(1), 257-261.

Sherekar, S., Thakare, V., Jain, S., Miss Ashwini, D. B., Tijare, P., Deshpande, M. S. A. (2011). Attacks and Countermeasures on Digital Watermarks: Classification, Implications, Benchmarks. *International Journal Of Computer Science And Applications.* 4(2).

Zhu, J., Wei, Q., Xiao, J., and Wang, Y. (2009). A fragile software watermarking algorithm for content authentication. *2009 IEEE Youth Conference on Information, Computing and Telecommunication, YC-ICT2009, September 20, 2009 - September 21, 2009*. Beijing, China: 391-394.