Journal of Information Assurance and Security 2 (2007) 297-302

Proposed Secure Mechanism for Identification of Ownership of Undressed Photographs or Movies captured Using Camera Based Mobile Phones

Samir B. Patel[1] and Shrikant N. Pradhan[2]

[1]AES Institute of Computer Studies, H.L. College Campus,
P.B. No. 4206, Navrangpura, Ahmedabad-380 009, Gujarat, India.
samir_mece@yahoo.com, sbpatel@aesics.ac.in

[2]Nirma Institute of Science and Technology, Department of Computer Science and Engineering, Nirma University,
Sarkhej-Gandhinagar Highway, Ahmedabad, Gujarat, India.
snp.it@nirmauni.ac.in

Abstract: Cameras attached to mobile phones are becoming more and more common, and as we move towards 3G and Next Generation Networks, it has become more a standard feature of mobile phones. Over recent months there have been a few grandiose claims within the media about the potential misuse of phones with camera capability. Unfortunately some of these claims are not proved by available facts resulting into confusion and misunderstanding. It may suffice to say that some digital cameras are smaller, convenient and technology superior in image quality. This makes them easier to use in an unacceptable manner.

Camera phones are designed to provide a means of transferring images via your mobile phone to complement voice or text based communication for business or personal reasons. Normally the youth gets attracted towards the sexual photography and watching movies on the mobile devices. Some times such movies get broadcast on the network like wild fire and it is available to all the community. It is indeed a difficult task to identify the user who has captured these photographs or movies and made it public. This paper focuses on a technique through which this problem can be solved. This technique, if implemented, on a mobile phone can really help the concerned authority to identify the culprits.

Keywords: Steganography, DCT, LSB, Digital Watermarking.

1. Introduction

It is necessary however to ensure that our young people are provided with sufficient guidance to make their own decision on what is appropriate to distribute via wireless networks and what the consequences could be if they allow themselves to be photographed in a situation where they could be blackmailed or embarrassed. Normally it is

not the responsibility of the service provider to monitor

all the information flowing on to the network. So there is a need for a secure mechanism to identify the owner of mobile device without his or her knowledge. Ultimately this mechanism has to be kept secret from the user community because if the user knows about such a mechanism which is included in a mobile device then it may adversely affect the business of the mobile manufacturer.

2. Mobile Phone Usage and Applications

Mobile phones are now as much a part of our lives as computers and the Internet as a means of communication. They are more in use than fixed line phones. They provide telecommunications to people remotely and in wireless manner providing more freedom for people to communicate. Mobile telecommunications can help us live our lives more efficiently. They cut down the need to travel, reduce business costs and can be vital safety devices. And of course people enjoy using them, especially our youth. Most young people over the age of 14 or 15 years now either own, or have access to a mobile phone and most now consider them a fashion accessory.

Mobile phones have changed the way our young people communicate. Text messaging has taught them a

Received December 11, 2007.

whole new language. More importantly, mobile phones allow us, as parents, the comfort of knowing that we can contact our children at any time. We now have the assurance of knowing that when our children are out late at night, they no longer have to search for a payphone that works to contact us – they have their mobile phone and can always call us in an emergency. The financial cost of maintaining a mobile phone is generally low, if it is used responsibly, considering the value and convenience it provides to parents and children. As with all technology solutions, some risk arise to the end users of product and service offerings, particularly those that provide us with the ability to connect with the global community.

It must be stressed that these risks are not new; they are simply applicable to a new operating environment. While most of us have a strong desire to enrich our lives by participating in this bigger environment, it is important that we are aware of the risks of mobile phone ownership. These risks range from the financial risk of ownership through to that associated with personal safety and the release of personal information about ourselves when communicating with others. It is equally important that we educate our children about these risks.

3. Introduction to Steganography and Digital watermarking

Steganography and Digital watermarking is the art of sending message within the image such that the existence of the message is not known to the capturer. The goal is to avoid the perception of hidden message within the image during transmission. If there is suspicion then the goal is not satisfied. Steganalysis is the art of identifying and extracting such covert messages.

Cryptography and Steganography form the basis for a large number of digital watermarking concepts. The stego system is conceptually similar to the crypto system.

Figure 1 shows the overall representation of the stego system whereby a key is additional data needed for embedding and extracting. The Embedding function and the Extracting function are opposite to each other in the sense that reverse operation will take place in extracting the message than that of embedding the message in the cover object.

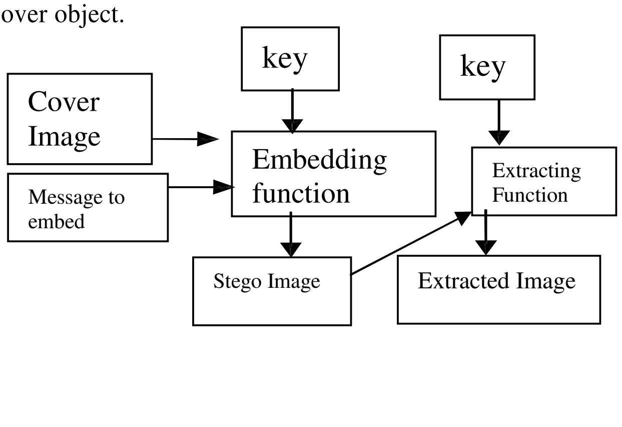


Figure 1: Block diagram of Stego System

Watermarking is very similar to steganography in a number of respects. Both seek to embed information inside a cover object with little to no degradation of the cover object. Watermarking however adds the additional requirement of robustness. An ideal steganography system would embed a large amount of information, perfectly securely with no visible degradation to the cover object. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness. Some methods of steganography and watermarking are as under.

- LSB (Least Significant Bit)
- Transformation based schemes

A major advantage of LSB algorithm is that it is quick and easy, whereas using transformation techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform(DWT) takes a large amount of time to embed and the embedding capacity is also less. There are number of other ways in which embedding can be carried out like redundant pattern encoding, spread spectrum method etc.

Applications: There is a growing importance of steganography and watermarking in intelligence work, as it is viewed as a serious threat to some governments, even the spying agencies can use it for the secret data transmission. Most researchers believe that steganography's niche in security is to supplement cryptography, not to replace it. Description like place, person's name, time, event, ownership, accessibility, etc. can be piggybacked with the original cover image/video/audio and retrieved at the destination end.

4. Steganography in Mobile Phone

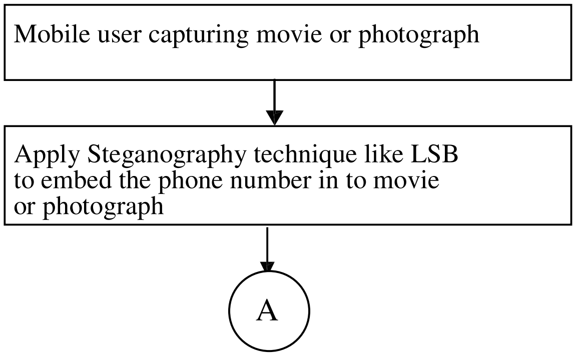
Steganography is the art of hiding information inside the cover object like image, audio or video, whereas adaptive steganography - an intelligent approach to hide messages through the techniques like LSB, Matrix Encoding and PN-Sequences - serves as a capable solution to recent security assurance concerns. Incorporating the above data hiding concepts with established cryptographic protocols in wireless communication would greatly increase the security and privacy of transmitting sensitive or non-sensitive information.

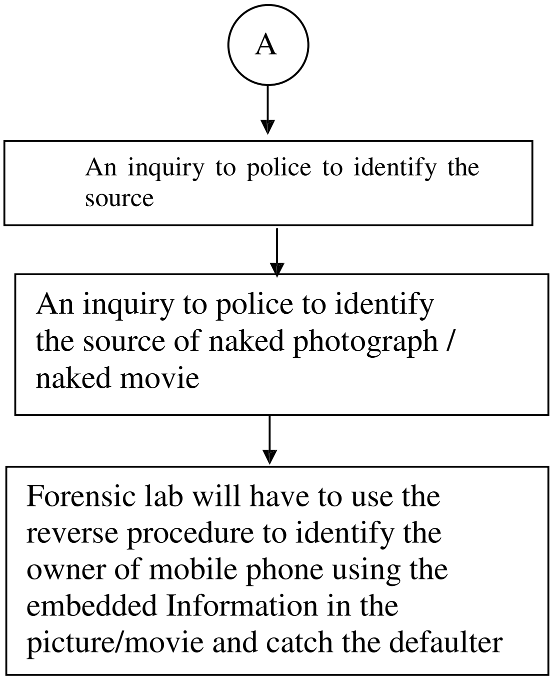
Here, I propose a model for identifying the owner of the mobile device who has taken the naked photographs or a movie through mobile phone. There are a number of issues that need to be resolved for embedding the information in the mobile phone like 1) low embedding capacity in mobile devices due to fixed image dimensions and memory constraints and 2) compatibility between mobile and land based desktop computers. There are number of applications which include steganography for secure banking applications. In this paper, I have tried to present a model to catch the owner of the mobile device who has taken the undressed movie/photographs.

The proposed concept is as follows:

- Photo or movie is captured by the user
- The phone number or mobile machine ID (Serial ID) is then embedded in the captured image/movie.
- The embedding algorithm which is applied at this point has to be very fast and the capacity of embedding also has to be considered. It must be possible to embed the information multiple times so that even though if some attack takes place intentionally/un-intentionally at the destination or in between then the information can be extracted error free.
- The embedding of information in to the image or movie should not have any artifacts on the captured image/movie.
- The simplest algorithm is Least Significant Bit insertion (LSB) but an attack or modification of bits can result in the loss of the embedded information. However, since the algorithm and the mechanism have to be kept secret, there are very rare chances that any user will ever come to know about this mechanism.
- There are other data hiding techniques which focus on robustness of the hidden data rather than capacity of data. If the robustness is to be considered then such a technique can be classified as Digital watermark or else a simple steganography technique.
- If the user is taking undressed photographs/movies and if he/she claims that this photograph/movie is not taken by him/her then this mechanism can prove the owner of the mobile device and can catch the mobile owner for this offence.

Proposed Layout for Identifying the Owner of Mobile Phone is as under:


Mobile user capturing movie or photograph
Apply Steganography technique like LSB to embed the phone number in to movie or photograph
A


A
An inquiry to police to identify the source
An inquiry to police to identify the source of naked photograph / naked movie
Forensic lab will have to use the reverse procedure to identify the owner of mobile phone using the embedded Information in the picture/movie and catch the defaulter

5. Algorithms

Two locations *Bi(u1,v1)* and *Bi(u2,v2)* are chosen from the low/middle frequency region of DCT for comparison, we must choose the coefficient on the recommendation of JPEG quantization table such that they have identical values.

5.1 Algorithm for embedding using block based method, using comparison between low-band coefficients.

- Set minimum coefficient difference
- Set the size of the block in cover to be used for each bit in watermark
- Read in the cover object
- Determine the size of cover image
- Read in the message bits (Serial number of mobile phone)
- Reshape the message to a Vector
- Check that the message isn't too large for cover
- Pad the message out to the maximum message size with ones.
- Generate shell of watermarked image
- Process the image in blocks
    - Encode such that (5,2) > (4,3) when message(x) =0 and that (5,2) < (4,3) when message(x)=1

  - o Transform block using DCT
  - o If message bit is black(5,2) > (4,3) then we need to swap them
  - o If message bit is white (5,2) < (4,3) then no need to swap them.
  - o Now adjust the two values such that their difference >=K (min. coefficient difference)
    - o Transform block back into spatial domain
    - o Move to the next block. And at end move to the next row.
- Store the file on a mobile device.

5.2 Algorithm for recovery using block based method, using comparison between low- band coefficients.

- Set the size of the block in cover to be used for each bit in watermark
- Read in the watermarked object
- Determine the size of watermarked image
- Determine maximum message size based on cover object and block size
- Read in original watermark
- Determine the size of original watermark
- Process the image in blocks
  O Transform block using DCT
  O If dct_block(5,2) > dct_block(4,3)
  Then message(x) =0
  Else message(x) =1
  O Move to the next block at end of row move to next row
  O Reshape the embedded message
- Show the embedded content to the user.

6. Attacks on embedded message/watermarks

A watermarked image is likely to be attacked intentionally or unintentionally. Some intentional attacks include cropping, filtering, rotation, scaling etc. And unintentional attacks include compression, transmission noise etc. Summarization of these different types of attacks is as follows:

- Lossy Compression: Many compression schemes like JPEG and MPEG can potentially degrade the quality of data through irretrievable loss of data.
- Geometric Distortions: Geometric distortions are specific to images videos and include such operations as rotation, translation, scaling and cropping.
- Common Signal processing operations: They include the following:
  O D/A Conversion
  O A/D Conversion
  O Re-sampling
  O Re-quantization
  O Dithering distortion
  O Recompression
  O Linear Filtering such as high pass and low pass filtering
  O Non linear filtering such as median filtering
  O Color reduction
  O Addition of constant offset to the pixel values
  O Addition of Gaussian and Non Gaussian noise
  O Local exchange of pixels.
- Other intentional attacks are also possible like watermarking of watermarked image, forgery, etc.

7. How to Embed/Recover device ID in/from captured image/video using camera based mobile phone

In mobile operating system camera application is treated as any other normal application. We need to monitor this application continuously in order to embed device ID in the captured image/video. Every time a camera phone is switched on, the operating system should start an application which will monitor the camera application. As soon as this application detects any camera event, it should embed the device ID in the captured image/video. Whenever any image/video is to be examined it can be transferred to any computing device where the device ID recovery algorithm is already available.

8- A Implementation results of DCT based method

In MBCX (Mid band Coefficient Exchange) method where k is the difference in coefficient and B is the block size.

Mid frequency band results				
		LENA	MOON	CAMERA MAN
	K	PSNR	PSNR	PSNR
B = 8	10	2.12E+04	4.42E+04	1.80E+04
	50	2.41E+03	2.92E+03	2.45E+03
	200	183.4009	201.5846	190.9553
B = 16	10	1.17E+04	3.88E+04	8.43E+03
	50	5.32E+03	8.41E+03	4.81E+03
	200	624.7721	744.1055	6.37E+02

Table 1: DCT RESULTS FOR MID BAND

8-B Implementation results of DWT – based method of 1scale and 2 dimensions

Here k is the watermarking gain constant and embedding is done in HL and LH band.

DWT Result using PN sequence(HAAR)			
	LENA	MOON	CAMERA MAN
K	PSNR	PSNR	PSNR
0.2	4.5852E+04	5.0465E+04	4.8105E+04
0.5	9.0000E+03	1.0831E+04	9.4811E+03
1	2.3216E+03	3.0520E+03	2.4488E+03
2	5.8312E+02	8.2148E+02	6.3395E+02
10	2.5822E+01	3.8053E+01	2.9130E+01
50	4.8272E+00	4.3320E+00	4.8499E+00

Table 2: DWT Results for 1-scale and 2- dimensions

8- C Implementation results of DWT – based method of 2scale and 2 dimensions

DWT Result using PN sequence (HAAR)			
	LENA	MOON	CAMERA MAN
K	PSNR	PSNR	PSNR
0.2	1.0584E+05	1.1390E+05	1.1103E+05
0.5	3.2000E+04	3.5818E+04	3.3576E+04
2	3.0005E+03	3.0375E+03	2.44E+03
5	3.7190E+02	5.4171E+02	4.1143E+02
10	9.4006E+01	1.4112E+02	1.0727E+02

Table 3: DWT Results for 2-scale and 2- dimensions

All the results were obtained in Mat lab. Since DCT and DWT techniques takes more time the best way is to use nLSB approach to embed more information in the cover image.

9. Conclusion

Digital media offer several distinct advantages over analog media, such as high quality, easy editing, high fidelity copying. The ease by which digital information can be captured, duplicated and distributed has led to the need for effective copyright protection tools. Using mobile phone is very common and manufacturers are sure to offer number of utility services embedded in the mobile devices. Some of the functions that are likely to be performed by the mobile device are securing the house, controlling the access to PC, AC, Refrigerators, Door openers, Gate openers, Location Trackers, User monitoring systems, Online banking, Railway and Air ticket reservations, Browsing the web etc.

In this paper the author has identified an area where the mobile manufacturers can play an important role by implementing this technique through which the identification of the mobile device with which a undressed image/video was captured can be made easily. Further, using this information the owner can be recognized and can be apprehended using Geographic Information System (GIS) systems already in use with most of the governments.

10. Acknowledgement

I would like to thank all the members of AES ICS for providing regular support and inspiration for the work.

My special thanks go to
Shri Bipin V. Mehta (Director, AESICS), Shri Pratik K. Munshi (Assistant Professor, AESICS) and Ms. Vibha B. Patel (Assistant Professor, Nirma University).

11. References

[1] Rajmohan, ”Watermarking of Digital Images”, ME Thesis Report, Dept. Electrical Engineering, Indian Institute of Science, Bangalore, India, 1998.

[2] S.P.Mohanty, ”Watermarking of Digital Images”, Masters Project Report, Dept. of Electrical Engineering, Indian Institute of Science, Bangalore - 560 012, India, Jan 1999.

[3] B.Pfitzmann, ”Information Hiding Terminology”, Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.347-350.

[4] W. Bendor, et. al., ”Techniques for Data Hiding”, IBM Systems Journal, Vol.35, No.3 and 4, pp. 313-336,1996.

[5] B.M.Macq and J.J.Quisquater, ”Cryptography for Digital TV Broadcasting”, Proc. of the IEEE, Vol.83, No.6, June 1995, pp. 944-957.

[6] David Kahn, ”The History of Steganography”, Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1- 7.

[7] R.J. Anderson and Fabien A.P. Petitcolas, ”On the Limits of Steganography”, IEEE Journal on Selected Areas in Comm., Vol.16, No.4, May 1998, pp.474-481.

[8] R.J. Anderson, ”Stretching the Limits of Steganography”, Proc. of First Int. Workshop on Information Hiding, Cambridge, UK,

May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

[9] E. Franz, et. al., ”Computer Based Steganography”, Proc. First Intl. Workshop on Information Hiding, Cambridge, UK, May 30 - June 1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).

[10] F.A.P.Petitcolas, et al., ”Information Hiding - A Survey”, Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1062-1078.

[11] C.Cachin, ”An Information-Theoritic Model for Steganography”, Proc. of the 2nd International Workshop on Information Hiding, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in CS, Vol.1525, Springer- Verlag.

[12] S.Craver, ”On Public-Key Steganography in the Presence of an Active Warden”, Proc. of the 2nd International Workshop on Information Hiding, Portland, Oregon, USA, 15-17 Apr 1998, Lecture notes in Comp Sc, Vol.1525, Springer-Verlag.

[13] N.F.Johnson and Sushil Jajodia, ”Exploring Steganography: Seeing the Unseen”, IEEE Computer, Vol.31, No.2, pp.26-34, feb.1998.

[14] N.Paskin, ”Towards Unique Identifiers”, Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1208-1227.

[15] K.Hill, ”A Perspective: The Role of Identifiers in Managing and Protecting Intellectual Property in the Digital Age”, Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1228-1238.

[16] P.B.Schneck, ”Persistent Access Control to Prevent Piracy of Digital Information”, Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1239-1250.

[17] D.Augot, et al., ”Secure Delivery of Images over Open Network”, Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1251-1266.

[18] M.D.Swanson, et al., ”Multimedia data Embedding and Watermarking Technologies”, Proc. of the IEEE, Vol.86, No.6, June 1998, pp.1064-1087.

[19] M.M.Yeung, ”Digital Watermarking”, Communications of the ACM, Jul.1998, Vol.41, No.7, pp.31-33.

[20] N.Memon and P.W.Wong, ”Protecting Digital Media Content”, Communications of the ACM, July 1998, Vol.41, No.7, pp.35-43.

[21] M.M Yeung, et al. ”Digital Watermarking for High-Quality Imaging”, IEEE First Workshop on Multimedia Signal Processing, June23-25 1997, Princeton, New Jersey, pp. 357-362.

[22] F. Mintzer, et.al., ”Effective and Ineffective Digital Watermarks”, IEEE Intl. Conference on Image Processing, ICIP-97, Vol.3, pp.9-12.

[23] J. Zhao, et. al., ”In Business Today and Tommorrow”, Communications of the ACM, July 1998, Vol.41, No.7, pp.67-72.

[24] J. M. Acken, ”How Watermarking Value to Digital Content?”, Communications of the ACM, July 1998, Vol.41, No.7, pp.75-77.

[25] S. Craver, et. al., ”Technical Trials and Legal Tribulations”, Communications of the ACM, July 1998, Vol.41, No.7, pp.45-54.

[26] F. Mintzer, et. al., ”Opportunities for Watermarking Standards”, Communications of the ACM, July 1998, Vol.41, No.7, pp.57-64.

[27] G.Voyatzis and I.Pitas, ”Protecting Digital Image Copyrights: A Framework”, IEEE Computer Graphics & Applications, Jan/Feb 1999, pp.18-24.

[28] C.Busch, et al., ”Digital Watermarking: From Concepts to Real-Time Video Applications”, IEEE Computer Graphics & Applications, Jan/Feb 1999, pp.25- 35.

[29] R. Mehul and R. Priti, “Discrete Wavelet Transform based Multiple Watermarking Scheme,” Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003.

[30] A Survey of Digital Image Watermarking Techniques Vidyasagar M. Potdar, Song Han, Elizabeth Chang presented at 2005 3rd IEEE International Conference on Industrial Informatics (INDIN)

Author Biographies

First Author: Samir B. Patel is born in Ahmedabad on 26/07/1975 he has done his engineering(BE Computer Engineering) from LD College of Engineering an d Master degree(ME Computer Engineering) from S. P. University and currently his pursuing his Ph.D. studies under the guidance of Dr. S. N. Pradhan from Nirma University. He has more than 10 years of academic experience. He is working in the capacity of assistant professor at AES Institute of Computer Studies, Ahmedabad.

Second Author: Dr. S. N. Pradhan is having a rich experience of more than 25 years of research at Phusical Research Laboratory, Ahmedabad. He is associated as the head of the department for MTech in Computer Science at Institute of Technology at Nirma University. He is guiding number of students at the Masters and Doctorate level.