Multimedia Contend Delivery System Based on Advanced Watermarking Algorithm

R.Durga Devi[1] S. Kalpana[2] V. Keerthana[3] A R. Kowshica[4] Vivek Pandiya Raj[5]
[1,2,3,4]Students [5]Assistant Professor
[1,2,3,4,5]Department of Computer Science & Engineering
[1,2,3,4,5]Vivekanandha College of Technology for Women, Tiruchengode, Tamilnadu, India,

Abstract— Wireless multimedia communications have developed rapidly with increasing wireless access bandwidth and popular intelligent devices. Recent, a number of studies have been conducted to design tough and well organized schemes for delivering multimedia content over error-inclined wireless networks. In contrast, very few of those studies have concentrated on the security aspect of such transmission. There is have been increasing demands for the security of wireless multimedia Applications in recent years. Wireless networks when compared to traditional wired networks, are more likely prone to malicious attacks. Current security methods include physical layer and application layer security technologies independently and separately. Typically, physical layer information is dynamic in wireless networks, and application layer information is related to wireless multimedia content delivery. Both of them have significant impact on security performance.

Keywords: Invisible Watermarking, Lossless Image Compression, AES

I. INTRODUCTION

Image Processing is a technique to enhance raw images received from cameras/sensors placed on satellites, space probes and aircrafts or pictures taken in normal day-to- day life for various applications. Various techniques have been developed in Image Processing during the last four to five decades. Most of the techniques are developed for enhancing images obtained from unmanned space crafts, space probes and military reconnaissance flights. Image Processing systems are becoming popular due to easy availability of powerful personnel computers, large size memory devices, graphics software etc.

Image Processing is used in various applications such as:

Remote, Sensing, Medical, Imaging, Non-destructive Evaluation, Forensic Studies, Textiles, Material Science, Military ,Film industry ,Document processing, Graphic arts, Printing Industry

II. METHODOLOGY

A. Multi-Level Image Water Marking (Sender) Mechanism

In this module, the image data is taken and encoded so that original image is changed. In addition, the type of the data (Normal/High definition) is also encoded. The encoded data is obtained as input, the source coding function encodes the contents according to the received input rate and required output rate. In the channel coding part, authentication and watermarking are constructed. First the data is packet, then encoded, followed by authorization and watermark in. The operations of authentication and water-marking can directly relate to the multimedia content since the application packet only depends on the multimedia content. As a result, the importance and priority of the packets can be obtained easily.

B. Multi-Level Image Water Marking (Receiver) Mechanism

At the receiver, sequences of packets are received. Then content detection is performed on the received content to test the integrity of the content. The packet errors are found out and the error report (feedback) from receiver to sender is being sent twice so that even if the first information is attacked, the second copy helps to recognize the error details. The original data is received and data type information is retrieved based on proper decoding. Based on the receiver capability, the Normal/High Definition data is find out. Then decoding occurs to get image data which contains original image with watermark data. Then de-watermarking is carried out, checked and raw image data is displayed if watermark found to be correct

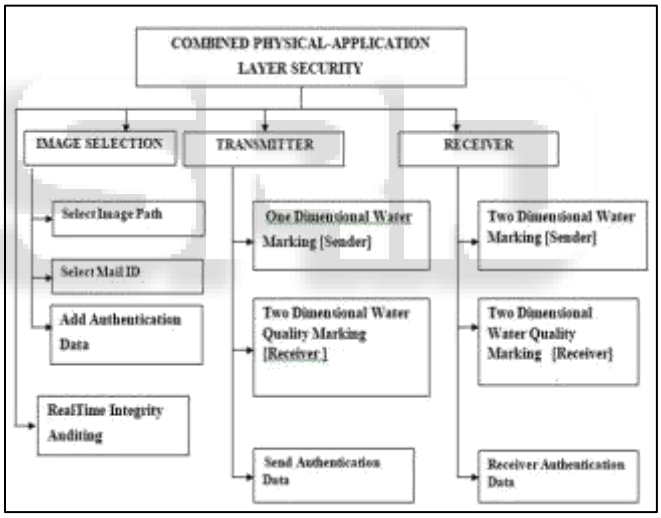


Fig. 2.1: Architecture Diagram

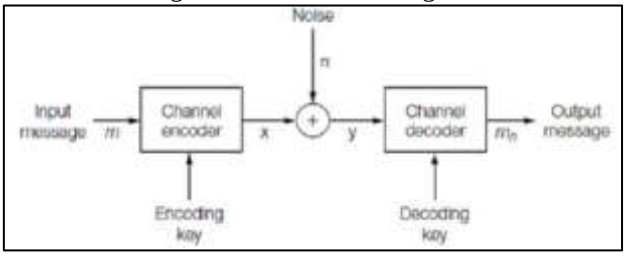


Fig. 2.2: Standard model of a communications

1) Watermarking Models

There are several ways in which we can model a watermarking process. These can be broadly classified in one of two groups. The first group contains models which are based on a communication-based view of watermarking and the second group contains models based on a geometric view of watermarking. In the rest of this essay, I only refer to image watermarking because I only concentrated on images during the development of example watermarking systems.

2) Communication-Based Models

Communication-based models describe watermarking in a way very similar to the traditional models of communication systems. Watermarking is in fact a process of communicating a message from the watermarking embedded to the watermarking receiver. Therefore, it makes sense to use the models of secure communication to model this process. In a general secure communication model we would have the sender on one side, which would encode a message using some kind of encoding key to prevent eavesdroppers to decode the message if the message was intercepted during transmission. Then the message would be transmitted on a communications channel, which would add some noise to the noise to the encoded message. The resulting noisy message would be received at the other end of the transmission by the receiver, which would try to decode it using a decoding key, to get the original message back.

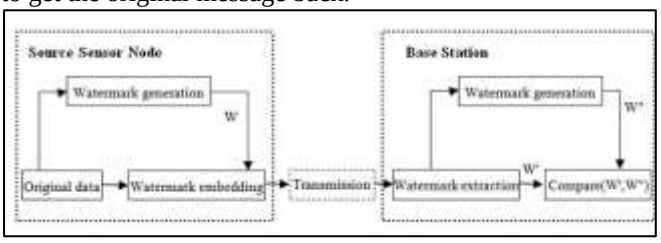
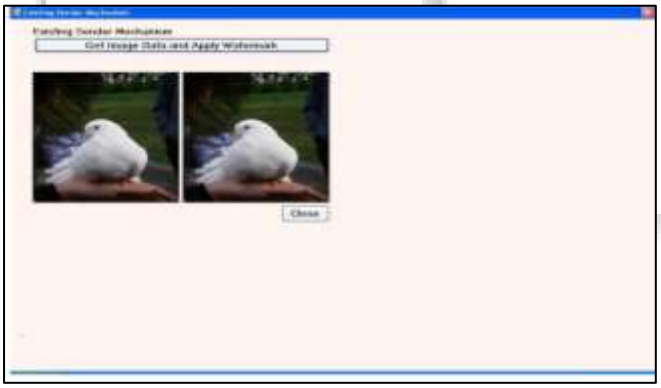
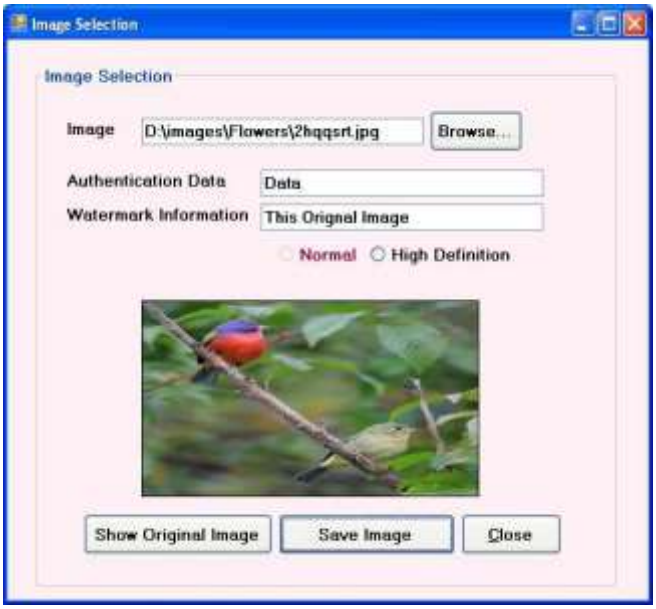
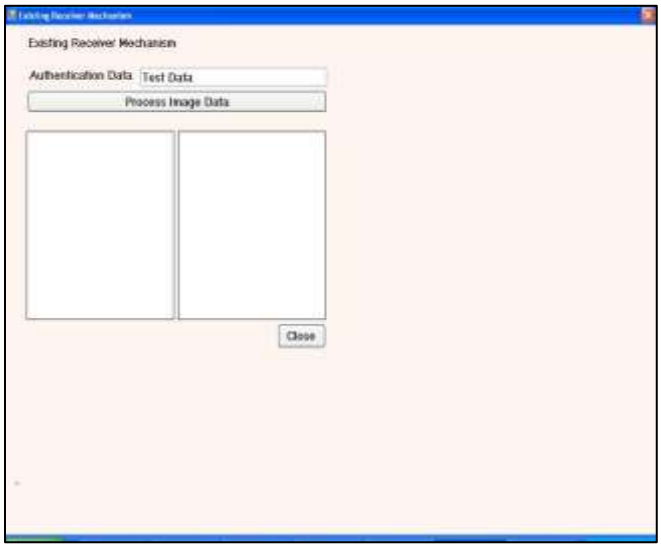


Fig. 2.3: Digital Watermark Embedding and Extraction Model



III. MODELING AND ANALYSIS





IV. RESULT AND DISCUSSION

FIELDNAME	TYPE	SIZE	DESCRIPTION
SNo	INT	4	Unique
Content	VARCHAR	50	Watermark content data

Fig 4.1 Login

1) Coding

Coding is the process of whereby the physical design specifications created by the analysis team turned into working computer code by the programming team.

2) Testing

Once the coding process is begin and proceed in parallel, program module can be tested.

3) Installation

Installation is the process during which the current system is replaced by the new system. This includes conversion of existing data, software, and documentation and work procedures to those consistent with the new system.

4) Documentation

It is result from the installation process, user guides provides the information of how the use the system and its flow.

Training and support

Training plan is a strategy for training user so they quickly learn to the new system. The development of the training plan probably began earlier in the project.

The best-suited application package to develop the system is Visual C# .NET under Windows environment.

B. Input Design

Input design is the process of converting user-originated inputs to a computer understandable format. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system. A large number of problems with a system can usually be tracked backs to fault input design and method.

The system takes input from the users, processes it and produces an output. Input design link that ties the information system into the world of its users. The system should be user-friendly to gain appropriate information to the user.

– To provide cost effective method of input.

- To achieve the highest possible level of accuracy.
- To ensure that the input is understand by the user.

C. System Testing

After the source code has been completed, documented as related data structures. Completed the project has to undergo testing and validation where there is subtitle and definite attempt to get errors. The project developer treads lightly, designing and execution test that will demonstrates that the program works rather than uncovering errors, unfortunately errors will be present and if the project developer doesn't find them, the user will find out. The project developer is always responsible for testing the individual units i.e. modules of the program. In many cases developer also conducts integration testing i.e. the testing step that leads to the construction of the complete program structure.

This project has undergone the following testing procedures to ensure its correctness.

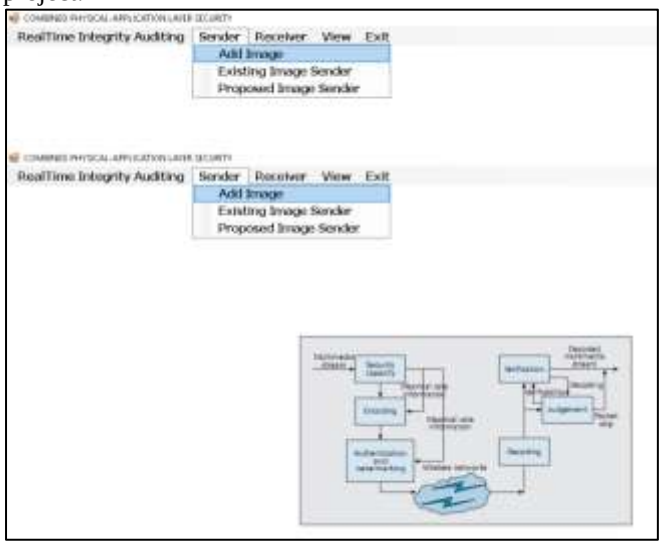
1) Unit testing
2) User Acceptance Testing

D. Unit Testing

In unit testing, we have to test the programs making up the system. For this reason, Unit testing sometimes called as Program testing. The software units in a system are the modules and routines that are assembled and integrated to perform a specific function, Unit testing first on the modules independently of one another, to locate errors. This enables, to detect errors in coding and logic that are contained with the module alone. The testing was carried out during programming stage itself.

E. User Acceptance Testing

In these testing procedures the project is given to the customer to test whether all requirements have been fulfilled and after the user is fully satisfied. The project is perfectly ready. If the user makes request for any change and if they found any errors those all errors has to be taken into consideration and to be correct it to make a project a perfect project.



F. Scope for Future Development

In future, more study will be carried out in following area.

- Device authentication: With the advances in the Internet of Things and device-to-device communications, the authentication of devices and their associated multimedia services should be verified jointly since different devices may have different multimedia content and security levels.
- Content confidentiality: The multimedia contents of the transmitters (e.g., devices), and the corresponding control and feedback messages should be more confidential to protect the privacy of both the transmitter and receiver.
- Green security: The receiver should be able to verify in an energy-aware way that any received contents are delivered unaltered in a multiple-user environment.
- Communication overhead: The cross-layer security service should be efficient in terms of communication and processing overheads because wireless multimedia communication is very sensitive to transmission latency

V. CONCLUSION

This project implements a joint framework involving both physical layer and application layer security technologies. Through exploiting the security capacity and signal processing technologies at the physical layer, and the authentication and watermarking strategies at the application layer, the available network resource can be efficiently utilized, and the scalable multimedia security service can be achieved without changing the current communication framework. Importantly, the proposed joint security architecture can be implemented in a distributed manner by exchanging messages between the authorized transmitters and receivers, thus achieving a satisfying trade-off between the security level and communication overhead. Based on the receiver capability, the Normal/High Definition data is found out. Then decoding occurs to get image data which contains original image with watermark data. Then dewater marking is carried out, checked and raw image data is displayed if watermark found to be correct

REFERENCE

[1] Y. Huang, Y. Gao, K. Nahrstedt, and W. He, "Optimizing File Retrieval in Delay-Tolerant Content Distribution Community," Proc. IEEE 29th Int'l Conf. Distributed Computing Systems (ICDCS '09), 2009.
[2] J. Reich and A. Chaintreau, "The Age of Impatience: Optimal Replication Schemes for Opportunistic Networks," Proc. Fifth Int'l Conf. Emerging Networking Experiments and Technologies (CoNEXT '09), 2009.
[3] V. Lenders, M. May, G. Karlsson, and C. Wacha, "Wireless Ad Hoc Podcasting," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 12, pp. 65-67, 2008.
[4] F. Li and J. Wu, "MOPS: Providing Content-Based Service in Disruption-Tolerant Networks," Proc. IEEE 29th Int'l Conf. Distributed Computing Systems (ICDCS '09), 2009.
[5] C. Boldrini, M. Conti, and A. Passarella, "ContentPlace: Social-Aware Data Dissemination in Opportunistic Networks," Proc. 11th Int'l Symp. Modeling, Analysis

and Simulation Wireless and Mobile Systems (MSWiM '08), 2008.
[6] M. Papadopouli and H. Schulzrinne, "A Performance Analysis of 7DS: A Peer-to-Peer Data Dissemination and Prefetching Tool for Mobile Users," Proc. IEEE Sarnoff Symp. Digest Advances in Wired and Wireless Comm., 2001.
[7] J.B. Tchakarov and N.H. Vaidya, "Efficient Content Location in Wireless Ad Hoc Networks," Proc. IEEE Int'l Conf. Mobile Data Management (MDM '04), 2004.
[8] A. Fast, D. Jensen, and B.N. Levine, "Creating Social Networks to Improve Peer-to-Peer Networking," Proc. 11th ACM SIGKDD Int'l Conf. Knowledge Discovery in Data Mining (KDD '05), 2005.
[9] A. Iamnitchi, M. Ripeanu, and I.T. Foster, "Small-World File-Sharing Communities," Proc. IEEE INFOCOM, 2004.
[10] M. Mcpherson, "Birds of a Feather: Homophily in Social Networks," Ann. Rev. Sociology, vol. 27, no.1, pp. 415-444 , 2001.
[11] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: vehicular content delivery using wifi," in MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking, 2008.
[12] D. T. J. Kangasharju, K.W. Ross, "Optimizing file availability in peer-to-peer content distribution," in INFOCOM 2007, 26th IEEE International Conference on Computer Communications, 2007.
[13] TIER Project, http://tier.cs.berkeley.edu/wiki/Home.
[14] RSS Advisory Board. RSS 2.0 Specification. http://www.rssboard.org/rss-specification, June 2007.
[15] M. Nottingham and R. Sayre (Eds.). The Atom Syndication Protocol. IETF RFC 4287, December 2005.
[16] B. Bloom. Space/time tradeoffs in hash coding with allowable errors. Communications of the ACM, 13(7):422–426, 1970
[17] P. Marshall. From self-forming mobile networks to self-forming mobile content services. ACM Mobicom Keynote Speech, 2008.
[18] H. Jafarpour, S. Mehrotra, and N. Venkatasubramanian. A fast and robust content-based publish/subscribe architecture. In Proc. of IEEE NCA, 2008.
[19] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau. CRAWDAD data set cambridge/haggle (v. 2006-09-15).
[20] http://crawdad.cs.dartmouth.edu/cambridge/haggle, September 2006.
[21] N. Eagle and A. Pentland. CRAWDAD data set mit/reality (v. 2005-07-01). http://crawdad.cs.dartmouth.edu/mit/reality, July 2005.
[22] M. Demmer, K. Fall, T. Koponen, and S. Shenker. Towards a Modern Communications API. In Proceedings of the 6th Workshop on Hot Topics in Networks (HotNets-VI), Atlanta, GA, November 2007
[23] G. Karlsson, V. Lenders, and M. May. Delay-tolerant broadcasting. In Proceedings of the 2006 SIGCOMM workshop on Challenged networks (CHANTS'06), pages 197–204, New York, NY, USA, 2006. ACM Press.
[24] L. Pelusi, A. Passarella, and M. Conti. Opportunistic Networking: data forwarding in disconnected mobile ad hoc networks. IEEE Comm. Magazine, 44(11), Nov. 2006.
[25] C. Boldrini, M. Conti, and A. Passarella. Exploiting users' social relations to forward data in opportunistic networks: the HiBOp solution. Pervasive and Mobile Computing (PMC), 2008.

