Control Theory and Informatics
ISSN 2224-5774 (Paper) ISSN 2225-0492 (Online)
Vol.5, No.1, 2015
www.iiste.org

Copyright Protection for Surveillance System Multimedia Stream with Cellular Automata Watermarking

Fahad Ahmad
School of Computer Sciences, National College of Business Administration & Economics, Lahore, Pakistan
fahadahmad84@gmail.com

Abstract
Intelligent Surveillance Systems are attracting extraordinary attention from research and industry. Security and privacy protection are critical issues for public acceptance of security camera networks. Existing approaches, however, only address isolated aspects without considering the integration with established security technologies and the underlying platform. Easy availability of internet, together with relatively inexpensive digital recording and storage peripherals has created an era where duplication, unauthorized use and misdistribution of digital content has become easier. The ease of availability made digital video popular over analog media like film or tape. At the same time it demands a sharp attention regarding the ownership issue. The ownership and integrity can easily be violated using different audio and video editing softwares. To prevent unauthorized use, misappropriation, misrepresentation; authentication of multimedia contents achieved a broad attention in recent days and to achieve secure copyright protection we embedded some information in audio and videos and that audio or video is called copyright protected. Digital watermarking is a technology to embed additional information into the host signal to ensure security and protection of multimedia data. The embedded information can't be detected by human but some attacks and operations can tamper that information to breach protection. So in order to find a secure technique of copyright protection, we have analyzed different techniques. After having a good understanding of these techniques we have proposed a novel algorithm that generates results with high effectiveness, additionally we can use self-extracted watermark technique to increase the security and automate the process of watermarking. Forensic digital watermarking is a promising tool in the fight against piracy of copyrighted motion imagery content, but to be effective it must be (1) imperceptibly embedded in high-definition motion picture source, (2) reliably retrieved, even from degraded copies as might result from camcorder capture and subsequent very-low-bitrate compression and distribution on the Internet, and (3) secure against unauthorized removal. Audio and video watermarking enables the copyright protection with owner or customer authentication and the detection of media manipulations. The available watermarking technology concentrates on single media like audio or video. But the typical multimedia stream consists of both video and audio data. Our goal is to provide a solution with robust and fragile aspects to guarantee authentication and integrity by using watermarks in combination with content information. We show two solutions for the protection of audio and video data with a combined robust and fragile watermarking approach. The first solution is to insert a time code into the data: We embed a signal as a watermark to detect gaps or changes in the flow of time. The second solution is more complex: We use watermarks to embed information in each media about the content of the other media. In our paper we present the problem of copyright protection and integrity checks for combined video and audio data. Both the solutions depend upon cellular automata, cellular automata are a powerful computation model that provides a simple way to simulate and solve many difficult problems in different fields. The most widely known example of Cellular Automata is the Game-of-Life. Cellular automaton growth is controlled by predefined rule or programs .The rule describes how the cell will interact with its neighborhood. Once the automaton is started it will work on its own according to the rule specified.

1. Introduction

Surveillance System

CCTV surveillance systems are now seen as a major tool for monitoring activities. The recent interest in surveillance in public, military and commercial scenarios is increasing the need to create and deploy surveillance systems. The increasing demand for security by society leads to a growing need for surveillance activities in many environments. Lately, the demand for remote monitoring for safety and security purposes has received particular attention, especially in the following areas: Transport applications such as airports maritime environment, railways, underground, and motorways to survey traffic. Public places such as banks, hospitals, supermarkets, homes, department stores and parking lots. Remote surveillance of human activities or other activities. Surveillance to obtain certain quality control in many industrial processes, surveillance in forensic applications and remote surveillance in military applications.

Copyright Protection

To handle this large amount of information and digital data obtained from surveillance system, issues such as scalability and usability (how information needs to be given to the right people at the right time) become very

important. The enforcement of distribution policies for sensitive intelligence digital documents is important but difficult. Sensitive documents may be found left behind in conference rooms, common areas, printing rooms or public folders in digital or paper format. Access control based on cryptography alone cannot address this problem. Once after obtaining access to a sensitive document may a person make redundant copies or handle it without care. A major challenge in the reinforcement of sharing policies for sensitive documents is the support of non-repudiation in the primary process so that unauthorized copies of intellect digital documents can be identified and traced back to their users.

Given these potential leaks, a content owner needs forensic tools that enable the tracking of unauthorized copies back to the party who licensed the use of the content, and who was responsible for preventing its further distribution. The ability of the content owners to identify the exact distribution point at which material was stolen can be used as a tool to identify the responsible parties and can act as a deterrent to such theft. A digital watermark uniquely identifying the licensee of that copy of the content can serve this purpose. This tracking watermark will give content owners a powerful forensic tool against piracy, because it allows them to trace pirated copies to the individual customers or to a specific post-production house, or to the time and location at which theft occurred.

Digital watermarking is recognized as a possible solution to this problem. It is the enabling technology to prove of ownership on copyrighted material, detect the originator of illegally made copies, monitor the usage of the copyrighted multimedia data and analyze the spread spectrum of the data over networks and servers.

Digital Watermarking

In the past few years, digital multimedia distribution over the Internet has grown rapidly as a result of the latest developments in technologies. Due to the continuously increasing availability of the Internet, the multimedia data can be easily shared, processed or used causing serious security problems. As a solution to this problem, different authentication techniques are used. However, the changes of digital information are always not being discovered because it is very easy to be modified and copied by the unauthorized copying and malicious tampering. Therefore, more attention is focused on the copyright protection of digital information. Digital watermarking technology is a field in computer science, cryptography and signal processing.

Conventional cryptographic schemes that cover only digital data are insufficient to handle this constraint. Thus to prevent this happening we need a copyright protection. In case of digital data we need the powerful copyright technique which is watermarking. Digital watermarking is a promising technology employed to achieve security purpose. It supports copyright information (such as the owner's identity, transaction dates, and serial numbers) to be embedded as unperceivable signals into digital contents. The signals embedded can be perceivable or insignificant to humans. The laws of copyright are designed to prevent this happening. The piracy of software, images, video, audio, and text has long been a concern for owners of these digital assets. Protection schemes are usually based upon the insertion of digital watermarks into the data.

The watermarking introduces small errors into the object being watermarked. These intentional errors are called marks, and all the marks together constitute the watermark. Digital watermarking is the process of adding information into multimedia data also called original media. The digital watermarking techniques are used to protect the digital data from illegal copying by embedding some information into the multimedia. A watermark is embedded into the host signal (e.g. - image, video, audio) that can be extracted later to verify identity of the owner. Digital video watermarking can be of two types – visible watermarking and invisible watermarking. In case of visible watermarking, the logo or the information appears in the video frames being completely visible or partially visible. In invisible watermarking, the information should not appear in the video i.e., it must be perceptually invisible. The invisible watermarking provides more security to video, though the visible watermarks protect the digital data in more active manner. Watermarking techniques can be classified as- Spatial domain and Frequency domain Watermarking Techniques. Spatial domain techniques can be Correlation based where different correlation properties are used such as adding noise, or adding pixels and Least Significant Bit whereas Frequency domain Watermarking Techniques are Discrete Cosine Transform, Discrete Wavelet Transform, Discrete Fourier Transform etc.

Invisible watermarking is hiding a message signal into a host signal, without any perceptual distortion of the host signal. Usually, the host signal is a digital media, like audio, video or images. Invisible video watermarking involves embedding watermark information into the frames those are derived from original digital video. Ideally, a user viewing the video cannot perceive a difference between the original, unmarked video and the marked video, but a watermark extraction application can read the watermark and obtain the embedded watermark.

The embedded signal can later be extracted or detected. The main challenge of watermarking is to achieve the trade-off among the low levels of distortion (imperceptibility), high robustness and high embedding capacity.

Consistent with those stated by SMPTE, a forensic watermark used for purchaser identification must

have the following properties.

- It must satisfy the high fidelity requirements of the content owners.
- Exhibition watermarks must be robust to the combination of exhibition capture and compression.
- Exhibition watermarks must be secure against unauthorized removal and unauthorized embedding.
- Embedding must fit into the process chain without adding undue delay. While latency may be acceptable, the embedding process should be as fast as the preceding process.

Cellular Automata

Cellular Automata (CA) are dynamical complex space and time discrete systems. They were originally proposed by Stanislaw Ulam and John von Neumann in the 1940s, as formal models for self-reproducing organisms. They consist of a certain number of identical cells, each of which can take one in a finite number of states. The cells are distributed in space in a rectangular grid, in one or more dimensions. At every time step, all the cells update their state synchronously by applying rules (transition function) which take as input the state of the cell under consideration and the states of its neighboring cells.

`1' – the A one-dimensional cellular automaton consists of two things: a row of "cells" and a set of "rules". Because of its inherent simplicity, the one-dimensional CA with two states per cell became the most studied variant of CA. There are also two-dimensional cellular automata, which use rectangular grids of cells. Each of the cells can be in one of several "states". The number of possible states depends on the automaton. Think of the states as colors. In a two-state automaton, each of the cells can be either black or white, the cells can change from state to state. The cellular automaton's rules determine how the states change. It works like this: When the time comes for the cells to change state, each cell looks around and gathers information on its neighbors' states. Based on its own state, its neighbors' states, and the rules of the CA, the cell decides what its new state should be. All the cells change state at the same time. Cellular automata on multi-dimensional grids have also been proposed. The grids have either null or periodic boundary.

In spite of their simple construction, CA can produce quite complex behavior, capable of generating useful operations. Wolfram has classified one-dimensional CA into four broad categories: (i) Class 1: ordered behavior; (ii) Class 2: periodic behavior; (iii) Class 3: random or chaotic behavior; (iv) Class 4: complex behavior [4]. CA with 'ordered' or 'periodic' behaviors are boring, in the sense that it is very easy to predict or describe what they do. On the other hand, 'random' or 'chaotic' CA is unpredictable and therefore not exciting. Somewhere in between, in the transition from periodic to chaotic, a complex, interesting behavior can occur. So far, CA have proved very powerful to simulate many real life applications and phenomena. It has also been proved that some (1-D) and (2-D) CA, such as the GL, are equivalent to the Universal Turing Machine.

Cellular Automata are widely used in different applications, such as art (generated images and music), random number generation, pattern recognition, routing algorithms and games. The application of cellular automata in the area of digital image processing includes image enhancement, compression, encryption and watermarking. The Game-of-Life (GL) is a Two Dimensional Cellular Automata (CA) that produces large amounts of patterned data. The ability to obtain complex global behavior from simple local rules makes CA an interesting platform for digital image watermarking

The rest of the paper is organized as follow. Section 2 discusses about category and essential properties of digital watermarking. Section 3 explaining implementation scheme and Spread- Spectrum technique of watermarking. We introduce proposed scheme (Stage Staffing Algorithm) in section 4 with detailed analysis of Logistic Map (chaotic map), 2-D Arnold Cat Map Technique and additional enhancement of security using DWT. Section 5 describing simulation results of proposed Stage Staffing Scheme and section 6, 7 are conclusion and future work respectively.

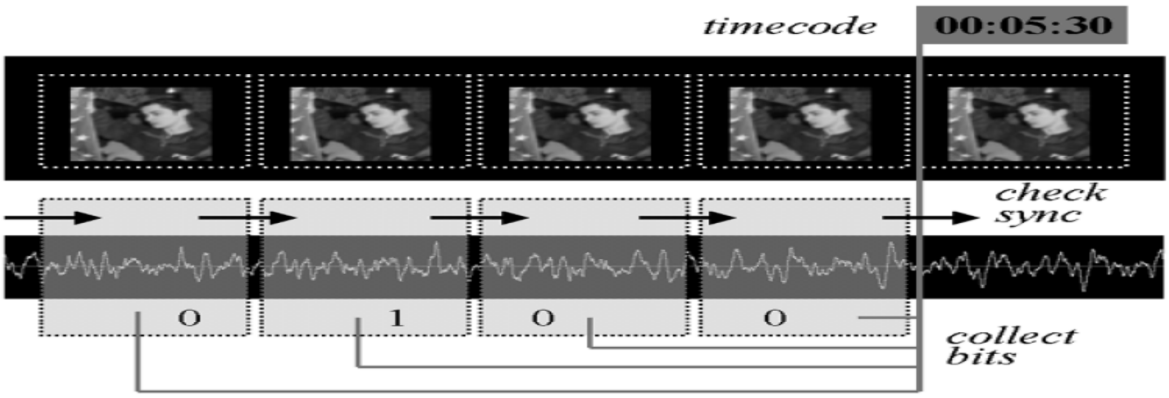
The embedding takes place by manipulating the content of the digital data that means the information is not embedded in the frame around the data.

2. Proposed Technique and Model

- **SYNCHRONISATION BASED APPROACH**

Inserting a time code into multimedia data is an efficient way to ensure integrity. If, for example, a part of an audio clip is erased, a gap in the retrieved time signals occurs, and the change is detected.

The most basic attack against the integrity of a multimedia stream or a combination of different multimedia is the removal of an unwanted small part. Another basic attack is the change of positions of parts of one stream while leaving the other as is, thereby attacking the synchronization of the streams. These attacks can be defeated by inserting time code information inside both media. Any removal of a frame or position changes can be used as structural attacks. They are detected because the flow of the timing signal is distorted.



The first design decision concerning synchronization schemes is to choose between absolute and relative time codes. An absolute time is a complete time stamp repeated over the signal, e.g. (00:00:00;00:00:01;...23:59:59) while a relative time code is a counter like on a tape deck using increasing numbers to generate specific accessible points in the recordings, e.g. (000,001,.., 999).

A well-known absolute synchronization time code is SMPTE (Society of Motion Picture and Television Engineers), which is used in video and music production. It offers a timing signal for a whole day (hh:mm:ss:ff, where f stands for frame) with a resolution down to single video frames. If a time code like SMPTE could be embedded in a multimedia stream as a watermark, every position in the stream would include complete timing information. Checking time integrity would be a simple task.

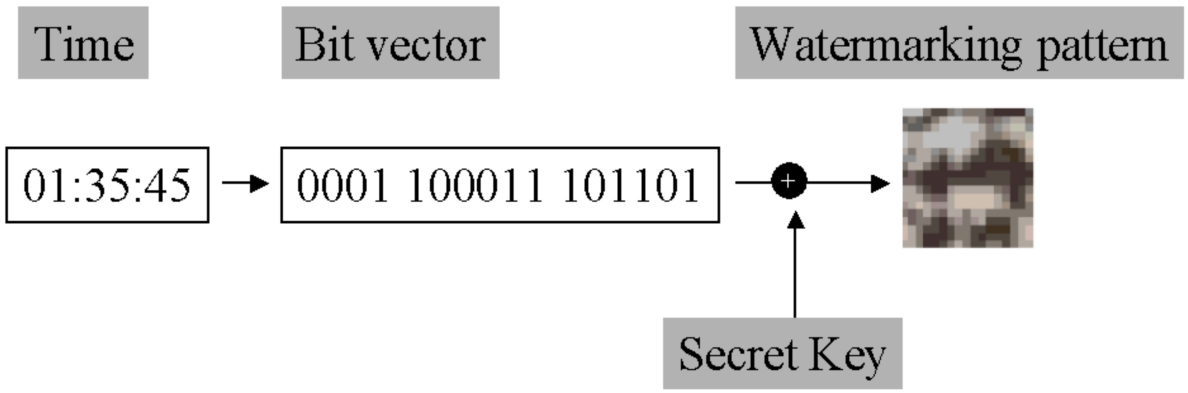
We use a time signal with dual synchronization properties. Figure 1 shows a video and an audio stream with embedded time codes. The embedded watermark works as an absolute time code like the one in the upper right corner of figure 1, while the data the watermark consists of is used as a relative time code. The absolute time code is used to synchronize the different media streams. It is encoded as a watermark using a secret key. No third party must be able to rewrite a time code after changing the content thereby obscuring attacks.

As robust watermarking technology is used to embed the absolute time code, very small parts of a media stream could be deleted without destroying the watermark. Very small changes cannot be detected. The second feature offers protection against this. Figure one shows that an absolute time code is embedded as a sequence of bits. The encoding parameters for these bits can be used as a relative time code if they are changed every time a bit is embedded. Figure 3 shows an example further described in section 2.2. When the time code is read, synchronization in the single media is checked for every bit of the watermark, and after retrieving the complete watermark, synchronization of the different media is checked.

Section 2.1 and 2.2 describe how this synchronization concept is realized for video and audio data. Two approaches are used. The time code for the video stream is used to initialize the watermarks to be embedded; the time code for the audio is the content of the watermark. The later one is a direct method while the first is an indirect one.

- **Synchronization Authentication with robust Video Watermarking**

Our used watermarking method in the video domain is based on overlaying a pattern with its power concentrated mostly in low frequencies. The pattern is created using a pseudo random number generator and a cellular automaton with voting rules.



We start by creating a 8x8 pseudo random pattern M with the time code and user key as a seed. To eliminate the

high frequencies in this pattern a cellular automaton with simple voting rules is used. Every position in the 8x8 random pattern is tested on the number of '1' in the eight co-sited positions. If the number exceeds five the actual position is set to '1' too, if the number is less than 3 it is set to '0', see the marked rectangle for an example. By applying these rules several times on the whole 8x8 block we obtain a pattern M with less high frequencies. Now a correlation between the pattern and the luminance block has to be inserted, we add the pattern to the luminance blocks of the image. We generate an 8x8 block to avoid visual distortions using a smooth-block/edge detector. Due to the fact that we use 8x8 patterns, we can embed the time code watermarking pattern redundantly to improve robustness against content-preserving operations. This redundancy can be used as a relative synchronization tool, as we will show in section 2.2.

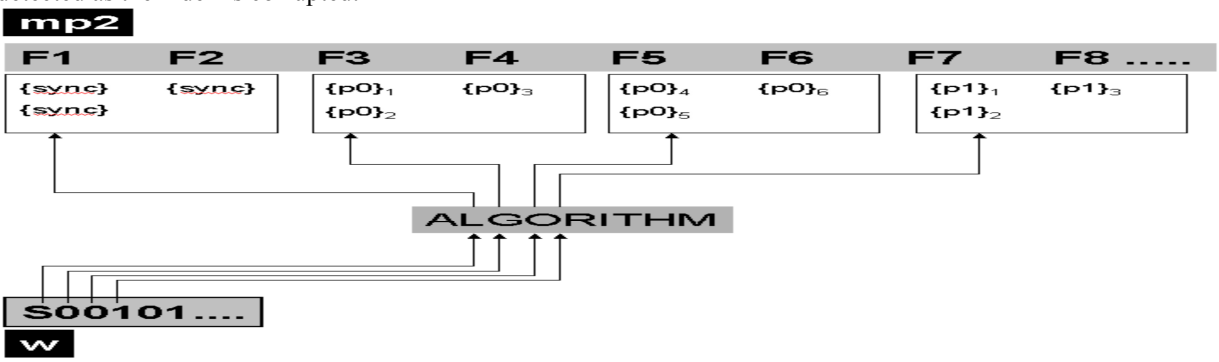
In the retrieval process the same 8x8 pattern M has to be generated as in the embedding process. To test the correlation between the luminance block and the pattern M the average luminance value *av1* of positions with a corresponding '1' and the average luminance value *av0* (sum0 div #0) with a corresponding '0' in the pattern M is produced. If the luminance block and the pattern M would be uncorrelated the difference of both values should be near zero. But due to the embedding process sum1 of these values should be significantly higher (around 2*k) than sum0. Thus we estimate an embedded pattern if *av1>av0*. Otherwise we estimate that this pattern was not embedded. With this statistical analysis we avoid using the original frames and can decide if the synchronization is correct or not to detect manipulations.

- **Synchronization Authentication with robust Audio Watermarking**

With a data rate of 16 bit per second we can embed a complete time code with a resolution of one second into the media.We introduce a method to embed a watermark with the dual synchronization properties mentioned above using our mp2- algorithm. It embeds watermarks into MPEG audio Layer 2 files using patterns in scale factors. Given a MPEG-file, a bit vector to embed and a secret key we encode the binary data into a sequence of patterns in the scale factors of the frames of the MPEG-file. Difference patterns based on this scale factors are calculated and the central algorithm changes these patterns until a sufficient number matches our desired sequence of patterns. The whole watermark is inserted in this way; if there are more frames than needed the watermark is inserted multiple times. Then the new scale factors are written in the source file, overwriting the old ones and so creating a watermarked MPEG-file.

We add another bit to the 16 time code bits for synchronization purposes, the sync-bit. This makes is easy to resynchronize when only a part of the watermarked file is available. During the retrieval of the watermark, the data bits are dropped until a synchronization bit is found. Our watermark to be embedded into one second of data will be w = (sync,{0,1}16). As we embed a watermark every second, this is the maximum time until a synchronization point is found. The pattern for the sync-bit stays the same over the whole file. The sequence of the following bits is encoded using a sequence of patterns instead of a fixed pattern as in the basic algorithm.

Figure 3 shows how the algorithm distributes the patterns over the frames. The watermark W consists of a synchronization bit (S) and a binary vector. The algorithm distributes it over the frames (F) of the MPEG file (mp2). Three different pattern types are used, {sync}, {p0} and {p1}, the latter two to embed the binary data. An index is given with the patterns to show how the algorithm uses different patterns {p0} and {p1} while embedding the complete time code. Even very small changes, e.g. dropping or swapping of frames, can now be detected as the index is corrupted.



5. Conclusion

Here in this paper we describe an approach to ensure the integrity of multimedia streams obtained through surveillance system using a combination of robust watermarking by embedding time code technologies. We discuss the weakness of existing watermarking solutions which usually concentrate on a single media type and explained the advantages of a mutual security concept.

Our concept of synchronization watermarking is a solution to protect the integrity of multimedia streams. We show how existing robust watermarking algorithms can be used to embed an absolute time code and also how to use redundancy as relative timing information.

In this technique we are including both visible and invisible watermark which gives an extra edge in the copyright protection. As we are using compound mapping to embed the visible watermark it helps to increase the robustness of the multimedia stream.

In this paper, a novel watermarking algorithm proposed to address the problem. Proposed algorithm is able to resist attacks of filtering, robustness. Processing operations such as, filtering, cropping, scaling, compression, rotation, randomly removal of some rows and columns lines, self-similarity and salt and paper noise.

6. References

[1] M. Yalcın, J. Vandewalle, P. Arena, A. Basile and L. Fortuna, "Watermarking on CNN-UM for Image and Video Authentication," *Wiley,* no. Watermarking, p. 31, 2004.

[2] J. Lubin, J. A. Bloom and H. Cheng, "Robust, Content-Dependent, High-Fidelity Watermark for Tracking in Digital Cinema," in *Electronic Imaging*, California, 2003.

[3] S. Das, P. Bandyopadhyay, S. Paul, P. A. Chaudhuri and D. M. Banerjee, "An Invisible Color Watermarking Framework for Uncompressed Video Authentication," *International Journal of Computer Applications,* vol. 1, no. Digital data watermarking, p. 7, 2010.

[4] S. Kumar, S. Kumar and S. Nandi, "Stage Staffing Scheme For Copyright Protection In Multimedia," *International Journal of Network Security & Its Applications,* no. Digital Watermarking Techniques, p. 13, 2011.

[5] H. WU, J. ZHOU, X. GONG and Y. W, "A Novel Image Watermarking Algorithm Using Dither Modulation in Cellular Automata Transform Domain," *Journal of Computational Information Systems,* no. Digital Watermarking, p. 8, 2011.

[6] O. ADWAN, A. AYYAL AWWAD, A. SLEIT and ABD, "A Novel Watermarking Scheme Based on Two Dimensional Cellular Automata," in *Recent Researches in Computers and Computing*, Amman,Tafila, 2008.

[7] P. Ghosh, R. Ghosh, S. Sinha, U. M, D. kr. kole and A. Chakroborty, "A Novel Digital Watermarking Technique for Video Copyright Protection," *Airccj,* no. Digital Watermarking, p. 9, 2012.

[8] J. Dittmann, M. Steinebach, I. Rimac, S. Fischer and R. Steinmetz, "Combined video and audio watermarking: Embedding content information in multimedia data," *citeseer,* no. Digital Watermarking In Multimedia, p. 10, 2000.

[9] J. Manoharan, D. C.Vijila and A. Sathesh, "Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks," *International Journal of Security,* vol. 4, no. 3, p. 10, 2010.

[10] M. Valera and . S. Velastin, "Intelligent distributed surveillance systems: a review," in *IEE*, Kingston, 2005.

[11] S. S. Bagade and V. K. Shandilya, "CELLULAR AUTOMATA AND WATERMARING FOR IMAGE COPYRIGHT PROTECTION," *International Journal on Computer Science and Engineering,* vol. 3, p. 4, 2011.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar