
ENCRYPTION ALOGRITHM WITH LARGE UNBREAKABLE KEY SPACE

INVENTION

The University of North Carolina at Greensboro is actively seeking parties interested in commercializing a method intended to secure and access information using multiple security as well as a system designed to ensure digital content security using a watermark.

The technology involves securing and accessing information using multiple security modules. It uses several different security elements in conjunction. The fact that the security system is nearly unbreakable makes it unique. It is a complete package in terms of processing speed, security and customization ability. It is indeed a 'one stop' solution for its users.

The system designed to ensure digital content security, uses fragile watermarking to secure the digital content. This invention overcomes the problems that current water marking schemes suffer as far as securing the electronic content is concerned.

APPLICATION

The invention that involves securing and accessing information using multiple security modules provides a comprehensive solution that is scalable both in terms of security and speed of processing. It could provide a 'one-stop' solution to businesses and enterprises looking for scalability combined with simplicity for varying kinds of information access and transmissions. It offsets the increased costs and risks associated with poor information protection and dissemination of critical data. Data leakage prevention (DLP) is another application that would benefit from this invention.

The primary invention which ensures digital security through watermarking technique uses a gradient image for key generation in order to watermark a digital image. This watermark is destroyed if the image is manipulated, even slightly.

ADVANTAGES

MULTIPLE SECURITY MODULE

The present invention offers features which majority of similar products designed to secure the digital content do not offer. Few of these features include the ease of integration, impact on processing speed, reliability and maintainability. Some major advantages of using the multiple security module are -

- It is faster because it can secure information transmitted over the internet without affecting the transaction speed.
- It is nearly unbreakable.
- It reduces the risks associated with poor information protection and dissemination of critical data.
- It provides protection against leakage of data.
- It makes the entire process of securing data very smooth.

WATERMARK

- A destroyed watermark can serve as an evidence that the image has been tampered with.
- It prohibits illegal downloading and sharing of video or any such digital content.
- The watermarking scheme provides high resistance to attacks, and if attacked, has a high probability of detection.
- It has the ability to detect, when an attacker attempts to modify an image without affecting the embedded watermark.

TECHNOLOGY

The recent technology represents a system for securing and accessing information using multiple security modules. This invention offers an algorithm for using several different security elements in conjunction—a key generator and encryptor-decryptor. The uniqueness of this invention is that the implementation can be customized to achieve a desired balance between the creations of secure cipher text with the desired transformation speed of plain text into cipher text.

The technology that uses watermarking is a novel algorithm that supports fragile watermarking through secure key generation. It provides an improved way to secure messages being transmitted between communicating devices. It has a multi-threading capability, thereby reducing the likelihood of a denial of service of attack.