



Article

Constructing of Digital Watermark Based on Generalized Fourier Transform

Ivanna Dronyuk ¹, Olga Fedevych ¹ and Natalia Kryvinska ^{2,*}

¹ Automated Control Systems Department, Lviv Polytechnic National University, 79013 Lviv, Ukraine; Ivanna.m.droniuk@lpnu.ua (I.D.); Olha.Y.Fedevych@lpnu.ua (O.F.)

² Department of Information Systems, Faculty of Management, Comenius University, 82005 Bratislava, Slovakia

* Correspondence: Natalia.Kryvinska@fm.uniba.sk

Received: 14 June 2020; Accepted: 6 July 2020; Published: 8 July 2020



Abstract: We develop in this paper a method for constructing a digital watermark to protect one-dimensional and two-dimensional signals. The creation of a digital watermark is based on the one-dimensional and two-dimensional generalized Fourier and Hartley transformations and the Ateb-functions as a generalization of trigonometric functions. The embedding of the digital watermark is realized in the frequency domain. The simulation of attacks on protected files is carried out to confirm the stability of the proposed method. Experiments proved the high stability of the developed method conformably to the main types of attacks. An additional built-in digital watermark can be used to identify protected files. The proposed method can be used to support the security of a variety of signals—audio, images, electronic files etc.—to protect them from unauthorized access and as well for identification.

Keywords: generalization of Fourier transform; Ateb-functions; digital watermark; data protection; signal processing

1. Introduction

In this paper, the method of constructing of digital watermark for one-dimensional and two-dimensional data arrays for the purpose of their protection and identification is developed. For their construction, the Ateb-functions are used, which are special functions that arise as analytical solutions of the differential equation of oscillatory motion with one degree of freedom.

The paper [1] describes methods for constructing stable digital watermarks (DWM) for image protection, in particular, based on Fourier transform. Digital watermarks are a part of technology for concealing information for protection purposes. In addition to the DWM, this technology also includes steganography. DWMs are divided into visible and invisible ones. The developed DWM based on Ateb transform is invisible, with embedding being implemented in the frequency domain. The authors of the monograph [2] show that the purpose of using digital watermarking technology is to control the intellectual property of data, data identification, and restrictions for the transmission of data in computer networks. The use of Ateb-functions in image protection tasks is considered in [3]. The paper [4] presents methods for data protection on tangible media using special functions. In papers [5,6], the importance of signal protection for video traffic was shown. The auto associative neural networks approach for the creation of a watermarking scheme is presented in [7]. All authors have denoted that the watermark methods are considerable.

The survey for constructing digital watermark schemes using singular-value decomposition is presented in [8]. The processing of hyperspectral images is considered in [9].

The article is an extended version of conference paper [10]. The main idea of the investigation is changing in the classical Fourier transform digital watermark schema [11] trigonometric functions into their generalization Ateb-functions and constructing Ateb-transform as generalization Fourier transform [12].

2. Materials and Methods

At the beginning of the article, we name the definition of Ateb-functions and prove some properties. Afterwards, a digital watermark constructing method based on Ateb-functions is considered. The proposed method is tested for many cases of attack. The results of experiments are shown in tables and figures. We discussed the obtained results, and finally, some conclusions are presented.

2.1. Definition of Ateb-Functions

The task of constructing a DWM based on the generalization of the Fourier transform in the form of Ateb-transform in order to protect and identify electronic data in the Internet is considered. To define the Ateb-transform, let us consider the definition of Ateb-functions. In [3], the properties of these functions are given in detail; therefore, only the most necessary definitions for the understanding of the further presentation are given.

Since the statement relates to special functions, it is known [13] that the incomplete beta function is determined by equation

$$B_X(p, q) = \int_0^x t^{p-1} (1-t)^{q-1} dt, \quad (1)$$

where p and q are real numbers. In a partial case, if $x = 1$, Equation (1) takes the form of the Euler integral of the first kind

$$B_1(p, q) = \int_0^1 t^{p-1} (1-t)^{q-1} dt, \quad (2)$$

i.e., the full Beta function.

All x values from interval $[0, 1]$ of functions $B_X(p, q)$ and $B_1(p, q)$ given by Equations (1) and (2), are positive and satisfy the conditions.

$$\begin{aligned} 0 &\leq B_X(p, q) \leq B_1(p, q), \\ B_X(p, q) &= B_1(p, q) - B_{1-X}(p, q). \end{aligned}$$

Consider the possible values for the parameters $p > 0, q > 0$, namely

$$p = \frac{1}{n+1}, \quad q = \frac{1}{m+1}; \quad (3)$$

where m and n are determined by the formulas

$$n = \frac{2\theta'_1 + 1}{2\theta''_1 + 1}, \quad m = \frac{2\theta'_2 + 1}{2\theta''_2 + 1}, \quad (\theta'_1, \theta''_1, \theta'_2, \theta''_2 = 0, 1, 2, \dots) \quad (4)$$

If $p > 0, q > 0$, then the Beta-function is definite and continuous, and for other valid values p and q , the function goes to infinity with $t \rightarrow 0$ or $t \rightarrow 1$. The mathematical definition of the Ateb-function is defined as an inversion to the Beta-function. Therefore, the name of the functions Ateb was proposed as the inversion of the word Beta.

Let us consider the expression

$$\omega = \frac{1}{2} \int_0^{-1 \leq y \leq 1} t^{-\frac{n}{n+1}} (1-t)^{-\frac{m}{m+1}} dt \quad (5)$$

where m, n are defined by Equations (5) and (4). Replacing the variables of the type

$$t = \bar{v}^{n+1}, \quad (6)$$

Equation (5) turns into a look

$$\omega = \frac{n+1}{2} \int_0^{-1 \leq \bar{v} \leq 1} (1 - \bar{v}^{n+1})^{-\frac{m}{m+1}} d\bar{v}. \quad (7)$$

In Equation (7), ω is a function from v , and also from m and n . To build Ateb-functions, let us consider the inverse dependence v from ω , which is a function m, n , is called Ateb-sine introduced in [14], and looks like

$$v = sa(n, m, \omega). \quad (8)$$

Similarly, the replacement of variables

$$t = 1 - u^{-m+1},$$

from Equation (1) get the ratio

$$-\frac{m+1}{2} \int_1^{-1 \leq u \leq 1} (1 - u^{-m+1})^{-\frac{n}{n+1}} d\bar{u} = \omega \quad (9)$$

Dependency u from ω for Equation (9) is a function of m and n and is called the Ateb-cosine and looks like

$$u = ca(m, n, \omega). \quad (10)$$

The basic relation for periodic Ateb-functions is

$$ca^{m+1}(m, n, \omega) + sa^{n+1}(n, m, \omega) = 1. \quad (11)$$

The Equation (11) is a generalization of the main trigonometric identity. Ateb-functions constructed for the values of the Equation (4) are periodic Ateb-functions. On the basis of these functions, analytic solutions of the system of ordinary differential equations are constructed

$$\begin{cases} \dot{x} + \beta y^m = 0, \\ \dot{y} + \alpha x^n = 0, \end{cases} \quad (12)$$

where α, β are some real constants.

If m, n satisfies the Equation (4), then Equation (12) describes oscillatory motion with one degree of freedom. The Ateb-functions are used successfully for modeling a vibration motion in [15,16]. However, in this investigation, we propose to use them for constructing a digital watermark.

From Equations (7) and (9), it is obvious that if $n = m = 1$, then there are received $u = \cos \omega$, $v = \sin \omega$. This property is the basis for the development of this study. Since Ateb-functions are a generalization of ordinary trigonometric functions, one can construct a generalization of the Fourier transform on the basis of these functions.

In the simulation and development of systems for the transformation and protection of information, methods based on the mathematical apparatus of orthogonal trigonometric transforms are widely used (OTT) [2]. A method of orthogonal transforms is proposed, which is based on periodic Ateb-functions. In the future, it will be called as an orthogonal Ateb-transform (OAT). The ability to build an OAT is based on such provisions. First, in [3,4], Ateb-functions are shown as a generalized case of ordinary trigonometric functions. Secondly, in [2], the orthonormality of a system of periodic Ateb-functions is

proved. In the works [3,4], the methods and algorithms for calculating Ateb-functions depending on the parameters have been developed, which allows successfully using the proposed method of OAT.

Let us introduce a generalization of the Fourier transform based on periodic Ateb-functions.

2.2. Construction of Orthogonal Ateb Transforms

In this section, continuous one-dimensional direct and inverse Ateb-transforms will be constructed first with one parameter, and then with two parameters.

Let us introduce the function of the Ateb-sine and cosine in the form $sa(n, 1, t)$ and $ca(1, n, t)$. Let $x(t)$ be a real function, then Ateb-transform will be the next

$$X(n, \omega) = A(n, \omega) - iB(n, \omega), \quad (13)$$

where

$$A(n, \omega) = \int_{-\infty}^{\infty} x(t) \cdot ca(1, n, \omega t) dt, \quad (14)$$

$$B(n, \omega) = \int_{-\infty}^{\infty} x(t) \cdot sa(n, 1, \omega t) dt. \quad (15)$$

Given the parity and the oddity of the Ateb-functions [3], let us write the inverse Ateb-transform in the form

$$x(t) = \frac{1}{2\Pi} \int_{-\infty}^{\infty} (A(n, \omega)ca(1, n, \omega t) - B(n, \omega)sa(n, 1, \omega t)) d\omega, \quad (16)$$

where Π is the half period of Ateb-functions. The right side of Equation (16) depends on the parameter n . For every value of n , the decomposition of function $x(t)$ will be different.

Character—that is, the rate of growth or decline of the period of the Ateb-functions $ca(1, n, \omega t)$ and $sa(n, 1, \omega t)$ —will vary depending on n . Dependence of the Ateb-function on the parameter n makes it possible to pick up the corresponding to $x(t)$ appearance of $ca(1, n, \omega t)$ and $sa(n, 1, \omega t)$, which corresponds to the task of constructing of security elements.

Let's introduce the Hartley function $csa(1, n, t)$ as

$$csa(1, n, t) = ca(1, n, t) + sa(n, 1, t). \quad (17)$$

Let's introduce straight and inverse Hartley Ateb-transform, using formulas

$$H(n, \omega) = \int_{-\infty}^{\infty} x(t) csa(1, n, \omega t) dt, \quad (18)$$

$$x(t) = \frac{1}{\Pi} \int_{-\infty}^{\infty} H(n, \omega) csa(1, n, \omega t) d\omega. \quad (19)$$

In case of $n = 1$ introduced by Equations (13)–(16), (18), and (19), Ateb transformations will be known as Fourier and Hartley orthogonal transforms. For the existence of the Ateb-transform function $x(t)$, it is sufficient to fulfill the same conditions that are sufficient for the existence of an orthogonal Fourier transform.

Let us consider that $x(t)$ is a real function; then, the analog of the known Fourier transform Ateb-transform will be constructed in the form

$$X(m, n, \omega) = A(m, n, \omega) - iB(m, n, \omega), \quad (20)$$

where

$$A(m, n, \omega) = \int_{-\infty}^{\infty} x(t) \cdot ca^m(m, n, \omega t) dt, \quad (21)$$

$$B(n, m, \omega) = \int_{-\infty}^{\infty} x(t) \cdot sa^n(n, m, \omega t) dt. \quad (22)$$

where $ca(m, n, \bar{\omega})$ is an Ateb-cosine function, and $sa(m, n, \bar{\omega})$ is an Ateb-sine function. Given the basic identity for the Ateb-functions in Equation (11), we obtain an expression for the inverse transform

$$x(m, n, t) = \frac{1}{\Pi} \int_{-\infty}^{\infty} \{A(m, n, \omega)ca(m, n, \omega t) + B(n, m, \omega)sa(n, m, \omega t)\} d\omega, \quad (23)$$

where $\Pi(m, n)$ is a half period of Ateb-functions. Let us take into consideration

$$casa(m, n, t) = ca^m(m, n, t) + sa^n(n, m, t). \quad (24)$$

Then, direct and inverse Hartley Ateb transforms will be written by formulas

$$H(m, n, \omega) = \int_{-\infty}^{\infty} x(t) casa(m, n, \omega t) dt \quad (25)$$

$$x(m, n, t) = \frac{1}{2\Pi} \int_{-\infty}^{\infty} H(n, \omega) casa(m, n, \omega t) d\omega \quad (26)$$

In case $n = 1, m = 1$ introduced by Equations (21)–(23), (25), and (26), Ateb-transforms will be known as orthogonal Fourier and Hartley transforms. Let us prove the validity of such properties for the introduced transforms: linearity, symmetry, similarity, displacement, modulation, and convolution, which are similar to the properties of ordinary Fourier and Hartley transforms.

2.3. Properties of One-Dimensional Orthogonal Ateb-Transforms

Lets deduce some properties of orthogonal Ateb-transforms. First, we consider the properties of one-dimensional orthogonal Ateb-transforms.

2.3.1. Property of Linearity

Let us consider that $x(t)$ is a linear combination of two other functions $x(t) = ax_1(t) + bx_2(t)$ than

$$X(n, \omega) = aX_1(n, \omega) + bX_2(n, \omega), \quad (27)$$

where $X(n, \omega)$ is a form of function $x(t)$, and $X_1(n, \omega), X_2(n, \omega)$ is a form of functions $x_1(t), x_2(t)$, respectively constructed according to Equation (13). The proof follows directly from the integral linearity.

A similar property is valid for the Hartley Ateb-transform

$$H(n, \omega) = aH_1(n, \omega) + bH_2(n, \omega), \quad (28)$$

where $H(n, \omega)$ is a form of function $x(t)$, and $H_1(n, \omega), H_2(n, \omega)$ is a form of functions $x_1(t), x_2(t)$ respectively for the Ateb-transform of Hartley, which is constructed according to Equation (25).

2.3.2. Property of Symmetry

The form of function $x(-t)$ is $X(n, -\omega)$ and $H(n, -\omega)$ accordingly. The proof follows from the properties of parity and oddity of Ateb-functions.

2.3.3. Property of Similarity

Consider the function $x(\frac{t}{T})$; then, the form of the function equals $|T| \cdot X(n, T\omega)$. A similar property for the Ateb-transform Hartley is the form of this function $|T| \cdot H(n, T\omega)$.

2.4. Properties of Two-Dimensional Orthogonal Ateb-Transforms

Let us consider some properties of orthogonal Ateb-transforms with two parameters.

2.4.1. Property of Linearity

Let the function $x(t)$ look like it is a linear combination of two other functions $x(t) = ax_1(t) + bx_2(t)$ than

$$X(m, n, \omega) = aX_1(m, n, \omega) + bX_2(m, n, \omega), \quad (29)$$

where $X(m, n, \omega)$ is a form of function $x(t)$, and $X_1(m, n, \omega)$, $X_2(m, n, \omega)$ is a form of function $x_1(t)$, $x_2(t)$, respectively constructed according to Equation (20). The proof follows directly from the linearity of the integral. A similar property is valid for the Hartley Ateb-transform.

2.4.2. Property of Symmetry

The forms of function $x(-t)$ are $X(m, n, -\omega)$ and $H(m, n, -\omega)$, accordingly. The proof follows from the properties of parity and oddity of Ateb-functions.

2.4.3. Property of Similarity

Let consider the function $x(\frac{t}{T})$; then, the form of function is equal to $|T| \cdot X(m, n, T\omega)$. A similar property for the Hartley Ateb-transform: the form of this function is $|T| \cdot H(m, n, T\omega)$.

2.5. Construction of the Digital Watermark

The need to increase the level of security of information transmission is connected with the new methods of creating, storing, and distributing information on paper carriers and with the change of the material carriers themselves, namely the introduction of plastic carriers of information, new types of paper, and other factors.

Therefore, raising the level of safety of documents on tangible media in the conditions of informatization of social processes is an urgent task. The original approaches for creating protection elements based on fractals are proposed in [9,10]. The efficient pre-processing procedure for images is developed in [17].

The development of methods of protection and identification in order to increase the level of security of documents and thus prevent violation of the integrity of information on tangible media to ensure the appropriate level of security of information transmission was also described.

Along with the development of new methods of protection, it is necessary to create new methods for identifying documents. In order to increase the level of security of printed documents by methods of graphical protection and identification in this work, the apparatus of the theory of Ateb-functions, in particular Ateb-transforms, is used. The work also describes the method of identifying a document based on the embedding of hidden information. A new method for identifying a document based on values of parameters m, n of Ateb-functions $f(m, n, x)$, and the introduced analogue of discrete orthogonal transformations are constructed.

To embed a hidden image, an additive algorithm was used using the discrete Ateb-transform (DAT), given by Equation (20) with different values of parameters m and n . An image conversion Equation (23) was used to read the image. The attached image or message is invisible because changes are made in a small number of elements, so the proposed method refers to the methods of hiding data in the frequency domain.

With DAT, let us convert the image and then use the following four ways to embed a hidden image [1]. In the first way, the r largest values are changed by the formula for embedding the hidden image in the form

$$z^{wp} = z^p + \alpha w, \quad (30)$$

where z^{wp} is the converted image, z^p is the original image, w is the hidden image size r , and α is the coefficient for adjusting the value of embedding.

In the second way, instead of Equation (28), let us use the next formula:

$$z^{wp} = z^p + e^{\alpha w}, \quad (31)$$

The third way is to apply the formulas of the form

$$z^{wp} = z^p + \alpha w, \quad (32)$$

To implement the fourth method, we use the formula

$$z^{wp} = z^p + \alpha w, \quad (33)$$

To verify the efficiency and stability of the proposed method of identification, the following experiments were carried out for parameter values $m = 3$, $n = 1/7$. Testing was performed for 10 standard images from the test base USC-SIPI, in particular for test images “LENA”, “BABUIN”, and others. The following series of attacks was carried out:

1. File resize 10%, 25%, 50%, 75%, 150%, and 200%;
2. Turn 1° , 5° , 10° , 45° , 90° , and 180° ;
3. Compress the image to 10%, 25%, or 50%;
4. Change the color depth of an image $256 \rightarrow 128$, $256 \rightarrow 64$, $256 \rightarrow 32$, $256 \rightarrow 16$, $256 \rightarrow 8$, $256 \rightarrow 4$, $256 \rightarrow 2$.

According to [1,7], these four types of attacks are the most common for images, when an image is not changing visually.

The criterion for the presence of a hidden image is correlation, which is calculated by the formula:

$$K = \frac{1}{r-1} \sum_{i=1}^r \frac{(c_i^w - \bar{c}_i^w)(w_i - \bar{w})}{\sigma_c \sigma_w} \quad (34)$$

where K is the correlation criterion, r is the hidden image size, c_i^w is the i -th image element, \bar{c}_i^w is the average value of image elements, w_i is the i -th hidden image element, \bar{w} is the average value of the hidden image elements, σ_c is the standard deviation of image elements with a hidden image, σ_w is the standard deviation of hidden image elements.

3. Results

If the calculated value K is larger than a given threshold value, it is assumed that the hidden image is present, and therefore the document is identified. Figure 1 shows the order of conducting experimental research. The results of experiments of identifying the presence of a digital watermark after the attacks with different coefficients of the value of the embedded image α by Equations (30)–(33) are presented in Tables 1 and 2. The << + >> sign is marked with the recognition of the embedded image, while the << - >> sign shows that embedded image is not found. Table 1 used Ateb-transforms with parameters $m = 1$, $n = 7$. Table 2 shows the results with parameters $m = 1/3$, $n = 1$. The given data demonstrate that the values of the parameters of the Ateb-functions have little effect on the results obtained. The values listed do not differ by more than 5%. In addition, the values obtained show that the best results are obtained for the parameter values $\alpha = 0.2$ and $\alpha = 0.5$. Tables 3 and 4 show the results of the recognition of the presence of a digital watermark after performing the attacks of converting a file format. In these tables, the Ateb-transform parameters used are the same as those in Tables 1 and 2; namely, in Table 3, parameters $m = 1$, $n = 7$ were used, and Table 2 shows the results with

parameters $m = 1/3$, $n = 1$. Conducted experiments showed that the proposed method is vulnerable to the conversion of the format tiff→jpg and persistent to the conversion to the jpg → bmp format.

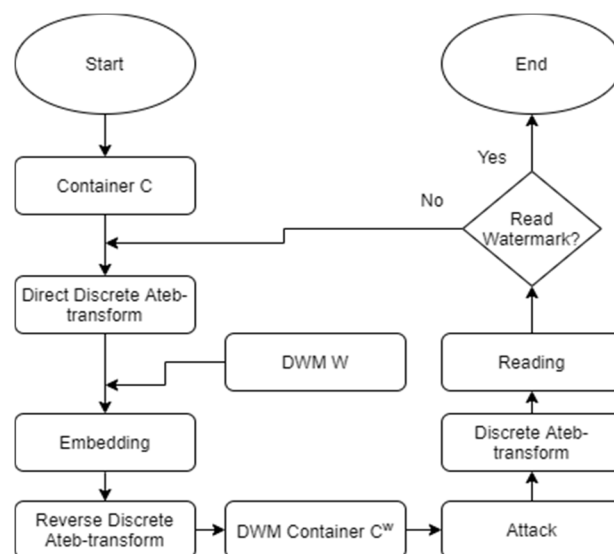


Figure 1. Flowchart for conducted experiments.

The study shows the comparison of the developed method with the known [1] method of constructing a digital watermark based on the Fourier transform. In [1], the data for the integral coefficient $\alpha = 0.2$ is given. That's why for comparison from Tables 1–4 the data are used only for $\alpha = 0.2$. Figure 2 shows data based on Table 1, and Figure 3 shows the data based on Table 3. To construct Figures 2 and 3, the ratio of the amount of positive recognition of a digital watermark to the total number of experiments of this species was calculated, and the result is given in percentage terms. Figure 2 illustrates the stability of the method compared with the known from [1] for attacks from Table 1. As can be seen, the developed method is much more stable than the previous, and in the case of a rotation attack, the image is stable in all 100% of cases, in contrast to the method in [1], which is stable only in 11% of the rotation attacks.

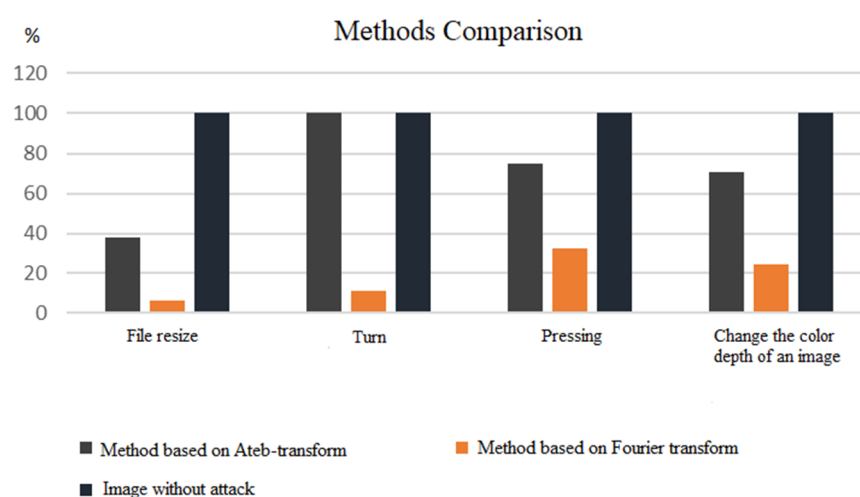


Figure 2. Comparison of the stability of methods for embedding a digital watermark in relation to attacks.

Figure 3 illustrates the stability of the method compared with the known from [1] for attacks from Table 3. Tables 5 and 6 show the results of the experiments of the conducted attacks of the type of format

conversion to verify the effectiveness of the method. It is shown that the developed method is more stable in three of the four attacks of file conversion compared with the known ones. For an attack to convert a file (jpg \rightarrow bmp), the method is stable in 100% of cases, and the method from [1] is only stable in 66% of the cases. However, for the converting attack (tiff \rightarrow jpg), the developed method is 100% vulnerable as well as the method discussed in [1]. As can be seen from the conducted experiments, the proposed method based on the DAT is resistant to most types of attacks. This proves the efficiency and stability of the proposed method. The method has a number of advantages over existing methods for the ratio of level of protection to the cost of organizing protection. For an attack to change the color depth, the results of the experiment are shown in Tables 1 and 2. Conducted experiments showed that the attack of the “change in color depth” image type does not affect the identification of the presence of a digital signature.

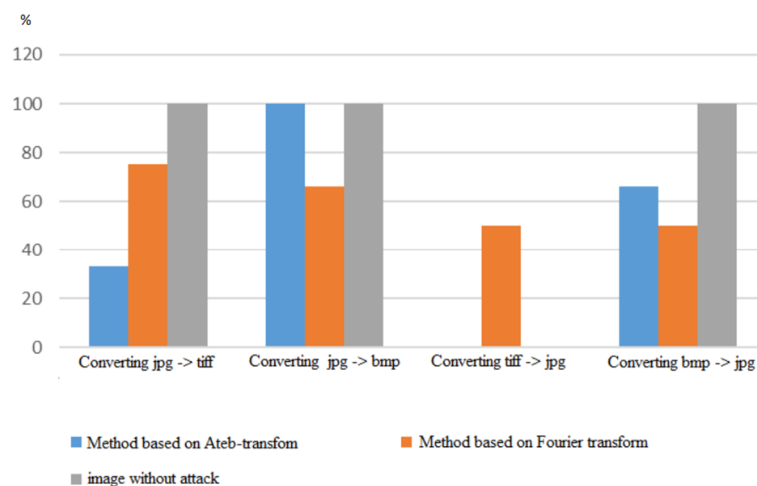


Figure 3. The stability of methods comparison for image format converting attacks.

Thus, the results of experimental studies on the application of the elaborated identification method were presented based on the embedding of hidden images described in this study, and these are effective in accordance with the parameters of stability and safety.

Table 1. The results of the experiments carried out on the attacks to verify the effectiveness of the method on the example of the test image “Lena” by Equation (34) for the parameters $m = 1$, $n = 7$.

Attack Type	File Sizing, %						Rotation Angle, °						
	Embed Ways	10	25	50	75	150	200	1	5	10	45	90	180
Without attack		+	+	+	+	+	+	+	+	+	+	+	+
Method 1, $\alpha = 0.1$		−	−	−	−	−	−	+	+	+	+	+	+
Method 1, $\alpha = 0.2$		−	−	−	−	−	−	+	+	+	+	+	+
Method 1, $\alpha = 0.5$		−	−	−	−	−	−	+	+	+	+	+	+
Method 1, $\alpha = 0.9$		+	+	−	−	−	−	+	+	+	+	+	+
Method 2, $\alpha = 0.1$		+	+	−	−	−	−	+	+	+	+	+	+
Method 2, $\alpha = 0.2$		+	+	−	−	−	−	+	+	+	+	+	+
Method 2, $\alpha = 0.5$		+	+	−	−	−	−	+	+	+	+	+	+
Method 2, $\alpha = 0.9$		+	+	−	−	−	−	+	+	+	+	+	+
Method 3, $\alpha = 0.1$		−	−	−	−	−	−	+	+	+	+	+	+
Method 3, $\alpha = 0.2$		−	−	−	−	−	−	+	+	+	+	+	+
Method 3, $\alpha = 0.5$		−	−	−	−	−	−	+	+	+	+	+	+
Method 3, $\alpha = 0.9$		+	+	−	−	−	−	+	+	+	+	+	+
Method 4, $\alpha = 0.1$		+	+	−	−	−	−	+	+	+	+	+	+
Method 4, $\alpha = 0.2$		+	+	−	−	−	−	+	+	+	+	+	+
Method 4, $\alpha = 0.5$		+	+	−	−	−	−	+	+	+	+	+	+
Method 4, $\alpha = 0.9$		+	+	−	−	−	−	+	+	+	+	+	+

Table 2. The results of the experiments carried out on the attacks to verify the effectiveness of the method on the example of the test image “Lena” by Equation (34) for the parameters $m = 1$, $n = 7$.

[illegible]

Table 3. The results of the experiments carried out on the attacks to verify the effectiveness of the method on the example of the test image “Lena” by Equation (34) for the parameters $m = 1/3$, $n = 1$.

Attack Type	File Sizing, %						Rotation Angle, °						
Embed Ways	10	25	50	75	150	200	1	5	10	45	90	180	
Without attack	+	+	+	+	+	+	+	+	+	+	+	+	
Method 1, $\alpha = 0.1$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 1, $\alpha = 0.2$	+	+	+	−	−	−	+	+	+	+	+	+	
Method 1, $\alpha = 0.5$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 1, $\alpha = 0.9$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 2, $\alpha = 0.1$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 2, $\alpha = 0.2$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 2, $\alpha = 0.5$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 2, $\alpha = 0.9$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 3, $\alpha = 0.1$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 3, $\alpha = 0.2$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 3, $\alpha = 0.5$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 3, $\alpha = 0.9$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 4, $\alpha = 0.1$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 4, $\alpha = 0.2$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 4, $\alpha = 0.5$	+	+	−	−	−	−	+	+	+	+	+	+	
Method 4, $\alpha = 0.9$	+	+	−	−	−	−	+	+	+	+	+	+	

Table 4. The results of the experiments carried out on the attacks to verify the effectiveness of the method on the example of the test image “Lena” by Equation (34) for the parameters $m = 1/3$, $n = 1$.

[illegible]

Table 4. Cont.

Embed Ways	Pressing Times, %			Change the Color Depth of the Image						
	10	25	50	128	64	32	16	8	4	2
Method 2, $\alpha = 0.1$	+	+	+	+	+	+	+	+	−	−
Method 2, $\alpha = 0.2$	+	+	+	+	+	+	+	+	−	−
Method 2, $\alpha = 0.5$	+	+	+	+	+	+	+	+	−	−
Method 2, $\alpha = 0.9$	+	+	+	+	+	+	+	+	−	−
Method 3, $\alpha = 0.1$	−	+	+	+	+	+	+	+	−	−
Method 3, $\alpha = 0.2$	−	+	+	+	+	+	+	+	−	−
Method 3, $\alpha = 0.5$	−	+	+	+	+	+	+	+	−	−
Method 3, $\alpha = 0.9$	+	+	+	+	+	+	+	+	−	−
Method 4, $\alpha = 0.1$	+	+	+	+	+	+	+	+	−	−
Method 4, $\alpha = 0.2$	−	+	+	+	+	+	+	+	−	−
Method 4, $\alpha = 0.5$	−	+	+	+	+	+	+	+	−	−
Method 4, $\alpha = 0.9$	+	+	+	+	+	+	+	+	−	−

Table 5. The results of the experiments of the conducted attacks of the type of format conversion to verify the effectiveness of the method on the example of the test image “Lena” by Equation (34) $m = 1$, $n = 7$.

Attack Type		Changing File Format			
Embed Ways	Converting Jpg → Tiff	Converting Jpg → Bmp	Converting Tiff → Jpg	Converting Bmp → Jpg	
Without attack	+	+	−	+	
Method 1, $\alpha = 0.1$	−	+	−	−	
Method 1, $\alpha = 0.5$	−	+	−	+	
Method 1, $\alpha = 0.9$	+	+	−	+	
Method 2, $\alpha = 0.1$	−	+	−	−	
Method 2, $\alpha = 0.5$	−	+	−	+	
Method 2, $\alpha = 0.9$	−	+	−	+	
Method 3, $\alpha = 0.1$	−	+	−	−	
Method 3, $\alpha = 0.5$	−	+	−	+	
Method 3, $\alpha = 0.9$	−	+	−	+	
Method 4, $\alpha = 0.1$	−	−	−	−	
Method 4, $\alpha = 0.5$	−	+	−	+	
Method 4, $\alpha = 0.9$	−	+	−	+	

Table 6. The results of the experiments of the conducted attacks of the type of format conversion to verify the effectiveness of the method on the example of the test image “Lena” by Equation (34) $m = 1/3$, $n = 1$.

Attack Type		Changing File Format			
Embed Ways	Converting Jpg → Tiff	Converting Jpg → Bmp	Converting Tiff → Jpg	Converting Bmp → Jpg	
Without attack	+	+	−	+	
Method 1, $\alpha = 0.1$	−	−	−	−	
Method 1, $\alpha = 0.5$	−	+	−	−	
Method 1, $\alpha = 0.9$	+	+	+	+	
Method 2, $\alpha = 0.1$	−	+	+	−	
Method 2, $\alpha = 0.5$	−	+	+	−	
Method 2, $\alpha = 0.9$	−	+	+	−	
Method 3, $\alpha = 0.1$	−	+	−	−	
Method 3, $\alpha = 0.5$	−	+	−	−	
Method 3, $\alpha = 0.9$	−	+	+	−	
Method 4, $\alpha = 0.1$	−	−	+	−	
Method 4, $\alpha = 0.5$	−	+	+	−	
Method 4, $\alpha = 0.9$	−	+	+	−	

4. Discussion

Thus, the results of experimental studies on the application of the elaborated identification method were presented; based on the embedding of hidden images described in this study, the results are effective in accordance with the parameters of stability and safety. The proposed method is new and belongs to the methods of protecting documents based on hiding data in the frequency domain. The novelty is the use of DAT based on Ateb-functions. A method of protection and identification has been developed to increase the level of security of documents in order to prevent the violation of the integrity of information on tangible media and to ensure the appropriate level of security of information transmission. The scope of DWM use is quite extensive; it covers electronic documents in computer networks. The scope of the use of the proposed method relates to the transmission of information in various organizations, where the necessary condition is the protection and identification of documents. The proposed method has been tested on image files, but it can be used to protect audio, video files, and electronic text documents. This indicates the relevance and practical significance of the proposed method.

The presented results of experimental studies on the application of the elaborated embedding scheme of the DWM, described in this study, are effective in accordance with the parameters of stability and safety. The proposed method is new and refers to the methods of concealing data in the frequency domain, which ensures the stability of the algorithm. The novelty is the application of the DAT, based on the mathematical apparatus of the Ateb-functions.

5. Conclusions

The method of constructing a digital watermark based on generalized Fourier transform for solving data protection problems on material carriers was developed. The construction of generalization is based on the use of Ateb-functions, which generalize the usual trigonometric functions. To construct the transform, the property of the orthogonality of the Ateb-functions is used.

A simulation of attacks and evaluation of the efficiency and stability of the method carried out on test images. A simulation of attacks of different kinds was carried out. In most cases, the method is stable. The most vulnerable is the conversion of some file formats.

A comparison of the developed method with the known method of constructing a digital watermark based on the Fourier transform has been conducted. The conducted experiments showed the greater stability of the method developed here.

Further research can be developed in the following areas:

1. Application of the presented Hartley transform to the creation of a digital water signature, and testing of its resistance to attacks based on the developed scheme of experiments;
2. Development, application, and research of the method of constructing a digital water signature based on the Ateb-cosine and Ateb-sine transform;
3. Research of the method of constructing a digital water signature on the basis of Ateb-transform for other types of images, in particular, for multispectral images;
4. Application of Ateb-transform parameters for the identification of data on electronic media;
5. Development, application, and research of the method of constructing a digital water signature based on one-dimensional Ateb-transform for sound files.

Author Contributions: Conceptualization, I.D.; methodology, I.D.; validation, N.K.; formal analysis, N.K.; investigation, O.F.; writing—original draft preparation, I.D. and O.F.; writing—review and editing, N.K.; supervision, N.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors thank the reviewers for the relevant comments that helped to present the paper better.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lipinski, P. *Odporne Cyfrowe Znaki Wodne w Obrazach: Adaptacyjny Dobór Dziedziny Osadzania*; Akademicka oficyna wydawnictwa EXIT: Warszawa, Poland, 2013; p. 221. (In Polish)
2. Sokil, B.I. Nonlinear oscillations of mechanical systems and analytical methods of their research. Diploma Thesis, Lviv Polytechnic National University, Lviv, Ukraine, 2001.
3. Dronyuk, I.M.; Nazarkevych, M.A. Development of modified amplitude-modulated screening method for improving printing quality. *Actual Probl. Econ.* **2014**, *4*, 455–461.
4. Dronyuk, I.M. *Technologies for Protecting Information on Tangible Media. Monography*; Lviv Polytechnic Publishing: Lviv, Ukraine, 2017; p. 200. (In Ukrainian)
5. Peleshko, D.; Ivanov, Y.; Sharov, B.; Izonin, I.; Borzov, Y. Design and implementation of visitors queue density analysis and registration method for retail videosurveillance purposes. In Proceedings of the 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 23 August 2016; pp. 159–162. [\[CrossRef\]](#)
6. Ivanov, Y.; Peleshko, D.; Makoveychuk, O.; Izonin, I.; Malets, I.; Lotoshunska, N. Adaptive moving object segmentation algorithms in cluttered environments. In Proceedings of the Experience of Designing and Application of CAD Systems in Microelectronics, Lviv, Ukraine, 24–27 February 2015; pp. 97–99. [\[CrossRef\]](#)
7. Tsybmal, Y.; Tkachenko, R. A digital watermarking scheme based on autoassociative neural networks of the geometric transformations model. In Proceedings of the 2016 IEEE 1st International Conference on Data Stream Mining and Processing, DSMP 2016, Lviv, Ukraine, 23 August 2016. [\[CrossRef\]](#)
8. Ahmadi, S.B.B.; Zhang, G.; Wei, S. Robust and hybrid SVD-based image watermarking schemes: A survey. *Multimed. Tools Appl.* **2020**, *79*, 1075–1117. [\[CrossRef\]](#)
9. Trunov, A.; Fisun, M.; Malcheniuk, A. The processing of hyperspectral images as matrix algebra operations. In Proceedings of the 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv, Ukraine, 20–24 February 2018.
10. Dronyuk, I.; Fedevych, O.; Demyda, B. Signals and images protection based on Ateb-transforms in infocommunication systems. In Proceedings of the 2018 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PICST, Lviv, Ukraine, 20–24 February 2018; pp. 461–464. [\[CrossRef\]](#)
11. Fares, K.; Amine, K.; Salah, E. A robust blind color image watermarking based on Fourier transform domain. *Optik* **2020**, *208*. [\[CrossRef\]](#)
12. Dronjuk, I.; Nazarkevich, M. A study on Ateb transform as a generalization of Fourier transform. *Curr. Trends Anal. Appl.* **2015**, 723–731. [\[CrossRef\]](#)
13. Abramowitz, M.; Stegun, I. Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables. Available online: http://people.math.sfu.ca/~{}cbm/aands/abramowitz_and_stegun.pdf (accessed on 14 May 2020).
14. Rozenberg, R.M. The Ateb(h)-functions and their properties. *Quart. Appl. Math.* **1963**, *21*, 37–47. [\[CrossRef\]](#)
15. Cveticanin, L.; Vujkov, S.; Cveticanin, D. Application of modified generalized trigonometric functions in identification of human tooth vibration properties. *Commun. Nonlinear Sci. Numer. Simul.* **2020**, *89*. [\[CrossRef\]](#)
16. Cveticanin, L.; Zukovic, M.; Cveticanin, D. Exact steady states of periodically forced and essentially nonlinear and damped oscillator. *Commun. Nonlinear Sci. Numer. Simul.* **2019**, *78*. [\[CrossRef\]](#)
17. Arena, P.; Basile, A.; Bucolo, M.; Fortuna, L. An object oriented segmentation on analog CNN chip. *J. IEEE Trans. Circuits Syst. I Fundam. Theory Appl.* **2003**, *50*, 837–846. [\[CrossRef\]](#)

