алгоритм построения цифровой подписи на эллиптической кривой над кольцом Z_q с выбором параметров криптосистемы. Это обусловлено тем, что все вычисления в этой криптосистеме можно производить в проективной системе координат с использованием системы остаточных классов, что позволяет существенно ускорить вычисления и повысить скорость работы криптосистемы.

Литература

1. Menezes A., van Oorchot P., Vanstone S. Handbook of applied cryptography. CRC press, 2. 1997. – 816 p.
2. Ростовцев А. Г. Маховенко Е. Б. Два подхода к логарифмированию на эллиптической кривой. http://www.ssl.stu.neva.ru/ssl/archieve/lift1.pdf
3. Gordon M. D. A Survey of Fast Exponentiation Methods // Journal of Algorithms, 27. 1998. – P. 129-146.
5. Menezes A., Okamoto T., Vanstone S., Reducing elliptic curve logarithms to logarithms in a finite field // IEEE Transactions on Information Theory, 39, 1993. – P. 1639-1660.

ALGORITHM OF THE DIGITAL SIGNATURE ON AN ELLIOTIC CURVE

Babenko M.G., Strekalov Y.A., Chervaykov N.I.

The existing algorithms of the digital signature on an elliptic curve are analyzed in article. Requirements for construction of algorithm of the digital signature on an elliptic curve over a ring Z_q are worked out, all calculations in it are made with use of system of residual classes.

Keywords: *elliptic curve, digital signature, cryptosystem, fields Galois, system of residual classes, discrete logarithm, singular and not singular curves.*

Бабенко Михаил Григорьевич, аспирант Кафедры «Высшая алгебра и геометрия» Ставропольского государственного университета (СГУ). Тел (8-8652) 38-80-84. E-mail: whbear@yandex.ru

Стрекалов Юрий Анатольевич, к.т.н., доцент Ставропольского филиала Поволжского государственного университета телекоммуникаций и информатики. (8-8652) 35-19-76. E-mail: sfpgati@yandex.ru

Червяков Николай Иванович, д.т.н., профессор, заведующий кафедрой «Прикладная математика и информатика» СГУ. Тел. (8-8652) 35-68-32, доб. 1154; 8 (8652) 35-48-61.

УДК 654.9

АЛГОРИТМ ОБРАБОТКИ ИЗОБРАЖЕНИЙ ПРИ ФОТОГРАММЕТРИЧЕСКИХ ИЗМЕРЕНИЯХ

Первунинских Д.В.

В статье рассмотрены специфика и варианты обработки изображений фотограмметрических измерений при съемке неметрической фотокамерой.

Ключевые слова: измерения; метрологические параметры; калибровка; фотограмметрия; неметрическая фотокамера; концевые меры; обработка изображений; программное обеспечение; стереомодель.

Введение

Наиболее часто при проведении фотограмметрических измерений используют стереоскопические фотоаппараты (неметрические фотокамеры). При этом делается два снимка одинаковыми объективами, выставленными в определенных направлениях.

Для вычисления результатов измерения в трехмерных координатах полагают следующие допущения [1]:

- точки размещения фотокамеры по горизонтальной оси симметричны ($x_1 = 0{,}5\ b$; $y = 0$; $z = 0$ и $x_2 = -0{,}5b$; $y = 0$; $z = 0$; b – расстояние между центрами осей фотоаппаратов при съемке);
- оптическая ось фотоаппарата параллельна вертикальной оси z измерительной системы координат;
- оси x и y систем координат снимка и измерительной системы совпадают;
- отсутствуют искажения геометрии изображения (дисторсия).

Координаты точки объекта x, y, z определяются из подобия треугольников [1] путем нахождения координат отображений u и v на первом и втором снимках.

$$u_1 = -f\frac{x - b/2}{z},\ v_1 = -f\frac{y}{z};$$
$$u_2 = -f\frac{x + b/2}{z},\ v_2 = -f\frac{y}{z}. \quad (1)$$

Решая систему уравнений (1), находим координаты точки объекта:

$$x = -\frac{1}{2}\cdot(u_1+u_2)\cdot\frac{z}{f} = \frac{1}{2}\cdot(u_1+u_2)\cdot\frac{b}{u_2-u_1};$$
$$z = \frac{b\cdot f}{u_2-u_1}; \qquad (2)$$
$$y = -v\frac{z}{f} = v\frac{b}{u_2-u_1}.$$

Разность $u_2 - u_1$ называется параллаксом точки; f – фокусное расстояние от центра объектива до плоскости изображения.

Постановка задачи

При использовании бытового фотоаппарата с неметрической камерой необходимо выполнить несколько снимков с разных положений и учесть координаты (XC, YC, ZC) и ориентацию (углы Эйлера: ω, κ, ϕ) фотоаппарата в пространстве.

Трехмерные координаты и система уравнений (1) трансформируются в систему координат (СК), связанную с положением фотоаппарата, номером снимка k и номером точки i:

$$u_{ik} = -f\frac{(X^i - X_C^k)m_{xx}^k + (Y^i - Y_C^k)m_{xy}^k + (Z^i - Z_C^k)m_{xz}^k}{(X^i - X_C^k)m_{zx}^k + (Y^i - Y_C^k)m_{zy}^k + (Z^i - Z_C^k)m_{zz}^k};$$
$$v_{ik} = -f\frac{(X^i - X_C^k)m_{yx}^k + (Y^i - Y_C^k)m_{yy}^k + (Z^i - Z_C^k)m_{yz}^k}{(X^i - X_C^k)m_{zx}^k + (Y^i - Y_C^k)m_{zy}^k + (Z^i - Z_C^k)m_{zz}^k}. \qquad (3)$$

Здесь коэффициенты m^k_{xx}, m^k_{xy}, m^k_{xz}, m^k_{yx}, m^k_{yy}, m^k_{yz}, m^k_{zx}, m^k_{zy}, m^k_{zz} – компоненты матрицы поворота M [2], определяемые углами ω^k, κ^k, ϕ^k:

$$\mathrm{M} = \begin{vmatrix} \cos\phi\cdot\cos\kappa & \cos\omega\cdot\sin\kappa + \sin\omega\cdot\sin\phi\cdot\cos\kappa & \sin\kappa\cdot\sin\omega - \cos\omega\cdot\sin\phi\cdot\cos\kappa \\ -\cos\phi\cdot\sin\kappa & \cos\kappa\cdot\cos\omega - \sin\omega\cdot\sin\phi\cdot\sin\kappa & \cos\kappa\cdot\sin\omega + \cos\omega\cdot\sin\phi\cdot\sin\kappa \\ \sin\phi & -\sin\omega\cdot\cos\phi & \cos\phi\cdot\cos\omega \end{vmatrix}.$$

Для определения координат различных точек на различных снимках необходимо осуществить преобразование СК. При преобразовании необходимо учитывать вид преобразования и измеренных параметров. В зависимости от этого различают следующие варианты.

1. Преобразование одной СК в другую с использованием следующих сочетаний различных шести параметров:

- начало координат (X_C, Y_C, Z_C) и углы Эйлера (ω, κ, ϕ) ориентации фотоаппарата в пространстве;
- вектор начала координат X и базисные вектора Ex Ez по осям x и z;
- углы ориентации ω, κ, ϕ в пространстве, определяющие матрицу поворота M [2].

2. Преобразование координат из внешней СК осуществляется [2] согласно системе уравнений:

$$x' = (x - X_C)m_{xx} + (y - Y_C)m_{xy} + (z - Z_C)m_{xz};$$
$$y' = (x - X_C)m_{yx} + (y - Y_C)m_{yy} + (z - Z_C)m_{yz}; \qquad (4)$$
$$z' = (x - X_C)m_{zx} + (y - Y_C)m_{zy} + (z - Z_C)m_{zz}.$$

Величины $m_{xx}, m_{xy} \ldots m_{zz}$ – компоненты матрицы поворота M [2]. В векторном виде $x' = \mathrm{M}(x - X_C)$; обратное преобразование $x = X_C + \mathrm{M}^T x'$.

3. Если две СК (СК1 и СК2) определены во внешней СК: (СК1: X_{C1}, M_1; СК2: X_{C2}, M_2), то преобразование из СК1 в СК2 будет иметь вид: $x'' = \mathrm{M}_2(X_{C1} + \mathrm{M}_1^T x' - X_{C2})$. Взаимосвязь СК2 и СК1 определяется: $\mathrm{M}_{2i}=\mathrm{M}_2\mathrm{M}_1^T$; $X_{C21}=\mathrm{M}_2(X_{C2}\, X_{C2})$. По компонентам матрицы M_{2i} определяются угловые параметры ориентирования ω_{21}, κ_{21}, ϕ_{21} при переходе из СК2 в СК1.

Измерения размеров объектов сводятся к определению координат изображений одних и тех же точек объекта на разных снимках и решению системы уравнений (3). Определяются трехмерные координаты точек объекта и положения фотоаппарата в момент съемки. Важным моментом при обработке информации является наличие необходимого числа опорных точек с известными трехмерными координатами.

Решение задачи

Рассмотрим возможные варианты решения системы уравнений (3) с известным f.

1. Изображения одной и той же точки предмета, измеренные на двух снимках с известными параметрами ориентирования X_C, Y_C, Z_C, ω, κ, ϕ дают 4 уравнения, по которым можно определить трехмерные координаты точки (X, Y, Z).

2. Три точки с известными трехмерными координатами, измеренными на одном снимке, дают 6 уравнений. Можно определить параметры ориентирования снимка X_C, Y_C, Z_C, ω, κ, ϕ (внешнее ориентирование снимка).

3. Для пары снимков можно выбрать общую внешнюю систему координат, в которой уравнения имеют простой вид (1)-(2) (базисная система координат); сами изображения приводятся в эту систему координат проективным преобразованием плоскости. Преобразованные изображения образуют стереопару, по ней удобно выполнять измерения, можно наблюдать стереоизображение. Базисную систему координат можно определить по известным параметрам внешнего ориентирования снимков X_C, Y_C, Z_C, ω, κ, ϕ.

4. Пять точек с неизвестными трехмерными координатами, измеренные на двух снимках, дают 5×2×2–5×3 = 5 уравнений. Можно определить угловые положения одного снимка относительно другого и, следовательно, положения снимков относительно базисной системы координат этой пары снимков с точностью до расстояния между точками съемки (взаимное ориентирование пары снимков). Положение базисной системы координат относительно СК объекта остается неизвестным. По связанной таким образом паре снимков можно выполнить трехмерные измерения с точностью до масштаба.

При использовании неметрической фотокамеры требуется учесть ее внутренние параметры:

- положение главной точки $u_{\text{М}}$, $v_{\text{М}}$, то есть проекцию оптического центра объектива на плоскость изображения (она не обязательно совпадает с центром кадра);
- реальные фокусные расстояния по вертикали и горизонтали кадра (неквадратные пиксели) $f_{\text{U}}, f_{\text{V}}$;
- нелинейные геометрические искажения, которые можно представить в виде разложения поправок по степеням измеренных на снимке координат [3-7]:

$$\begin{aligned} u' &= u + D_{U\_UUU}u^3 + D_{U\_UVV}uv^2 + \dots ; \\ v' &= v + D_{V\_VVV}v^3 + D_{V\_VUU}vu^2 + \dots , \end{aligned} \quad (5)$$

где D_{U_UUU}, D_{V_VVV} – коэффициенты дисторсии.

В данном случае необходимо решение системы уравнений:

$$\begin{aligned} & u_{ik} - u_{\text{М}} + D_{U\_UUU}u_{ik}^3 + D_{U\_UVV}u_{ik}v_{ik}^2 + \dots = \\ & = -f_U \frac{(X^i - X_C^k)m_{xx}^k + (Y^i - Y_C^k)m_{xy}^k + (Z^i - Z_C^k)m_{xz}^k}{(X^i - X_C^k)m_{zx}^k + (Y^i - Y_C^k)m_{zy}^k + (Z^i - Z_C^k)m_{zz}^k}; \\ & v_{ik} - v_{\text{М}} + D_{V\_VVV}v_{ik}^3 + D_{V\_VUU}v_{ik}u_{ik}^2 + \dots = \\ & - f_V \frac{(X^i - X_C^k)m_{yx}^k + (Y^i - Y_C^k)m_{yy}^k + (Z^i - Z_C^k)m_{yz}^k}{(X^i - X_C^k)m_{zx}^k + (Y^i - Y_C^k)m_{zy}^k + (Z^i - Z_C^k)m_{zz}^k}. \end{aligned} \quad (6)$$

Структура решения уравнений (6) может быть представлена в виде, показанном на рис. 1. Систему (6) предлагается решать по частям.

1. Калибровка фотокамеры. Требуемые параметры камеры определяются заранее по снимкам калибровочных объектов с известной геометрией, предполагается, что параметры камеры сохраняются во время рабочих измерений. Возможно уточнение параметров по рабочим снимкам.

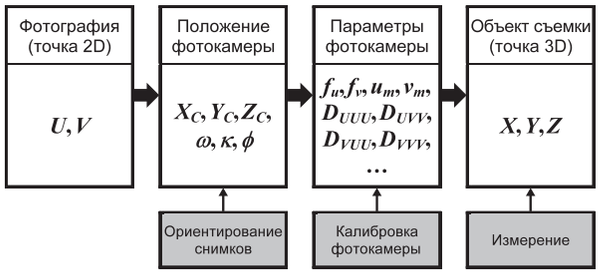

Рис. 1. Структура решения уравнений

2. Ориентирование снимков. Выполняется связывание снимков по известным опорным точкам и, возможно, по некоторым точкам измеряемого предмета. Используются хорошо опознаваемые и надежно измеряемые точки. Оценивается точность полученной стереомодели.

3. Измерение точек предмета. Для удобства измерений могут формироваться стереопары.

Заключение

В ходе работы были проведены измерения концевых мер вышеописанным способом. Концевые меры – это метрологические устройства, предназначенные для точного измерения геометрических размеров объектов, их метрологический параметр, в нашем случае – толщина, нормирован и подвергается периодической аттестации. Для проведения испытаний были взяты четыре типа мер с толщинами 6; 7; 8 и 9 мм. Тестовые объекты были сфотографированы в приспособлении, их фотографии подвергнуты обработке с помощью специального программного обеспечения (см. рис. 2). Контрольные точки устанавливались как на переднем плане фотоснимков, так и на заднем. Результаты измерений представлены в таблице 1.

Таблица 1. Результаты измерений концевых мер

	Мера «6»	Мера «7»	Мера «8»	Мера «9»
Размеры меры, мм	5,996	6,997	7,999	8,999
Результаты измерений, мм	6,005	7,080	7,958	9,092
Погрешность, мм	0,009	0,083	0,041	0,093

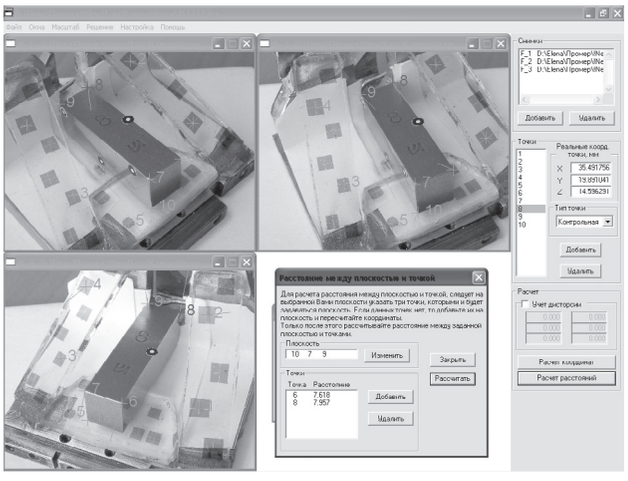

Рис. 2. Измерение концевых мер

Как видно из таблицы 1, погрешность измерения не превышает 100 мкм, что дает возможность использования подобных устройств для измерения размеров трехмерных объектов в оперативных условиях (например, при фиксации ДТП или летучем контроле деталей на производстве).

Литература

1. Mikhail E., Bethel J., McGlone J.C. Introduction to Modern Photogrammetry. Wiley&Sons Inc., 2001. – 450 p.
2. Первунинских Д.В. Перспективы использования триангуляционного метода определения размеров трехмерных объектов // Современные технологии безопасности. М.: Вып. 3(22), июль-сентябрь, 2007. – С. 31-32.
3. Назаров А.С. Фотограмметрия. М.: ТетраСистемс, 2006. – 360 с.
4. Форсайт Д. А., Понс Ж. Компьютерное зрение. Современный подход: Пер. с англ. М.: Вильямс, 2004. – 928 с.
5. Книжников Ю.Ф. Цифровая стереоскопическая модель местности. М.: Научный мир, 2004. – 244 с.
6. Русинов М.М. Инженерная фотограмметрия. М.: Недра, 1966. – 248 с.
7. Первунинских Д.В. Применение фотограмметрических триангуляционных методов в системах контроля и управления доступом // ИКТ. Т. 6. Спец. выпуск «Технологии безопасности и охраны», 2008. – С. 35-38.

IMAGE PROCESSING ALGORITHM DURING PHOTOGRAMMETRIC MEASUREMENTS

Pervyninskish D.V.

The article is devoted to the problem of specific character and variants of image processing of photogram-metric measurements during exposure with a non-metric camera.

Keywords: *measurements; metrological parameters; calibration; photogram-metric; non-metric camera; trailer measures; image processing; software; stereo-model.*

Первунинских Дмитрий Вадимович, заместитель начальника отдела НИКИРЭТ – филиала ФГУП «ПО «Старт» им. М.В. Проценко» (г. Пенза). Тел. (8-841) 265-48-23. E-mail: office@nikiret.ru

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 744.004.92

ПРИМЕНЕНИЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ОСНОВ ИННОВАЦИОННОГО ОБРАЗОВАНИЯ В ГРАФИЧЕСКИХ ПОСТРОЕНИЯХ ВИДОВ НА ЧЕРТЕЖАХ

Сапаров В.Е.

Предлагается метод построения видов (разрезов) на ЭВМ как альтернативный стандартному методу и методам, изложенным в учебниках, рекомендованных Министерством образования РФ. Проведена их сравнительная оценка с определением более рационального метода и эффективности его применения.

Ключевые слова: образование, компьютерные технологии, графические построения, правила, разрезы, проекции.

Международная организация ЮНЕСКО, входящая в структуру ООН, отмечает, что XXI век – это век образования. В сфере образования наметилась новая концепция – инновационное образование. Так, ключевой признак «решение типовой задачи» в существующей системе образования (поддерживающей) имеет только одно решение – «правильное», а по ключевому признаку «критерии оценки решения» – тоже только «правильно» или «неправильно».

В инновационном образовании эти ключевые признаки обуславливаются: для решения типовых задач – «множество (допустимых) решений» и для критерия оценки – «множество критериев» (полез-